Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Факультет Комп'ютерної інженерії та управління
(повна назва)
Кафедра Безпеки інформаційних технологій
(повна назва)

АТЕСТАЦІЙНА РОБОТА
Пояснювальна записка

рівень вищої освіти другий (магістерський)

Аудит інформаційної безпеки в комп'ютерних мережах на базі Mikrotik
(тема)

Виконав: Гавриленко А. С.
(прізвище, ініціали)
студент 2 курсу, групи БДІРм-18-1
Спеціальність 125 Кібербезпека
(код і повна назва спеціальності)
Тип програми освітньо-професійна
(освітньо-професійна або освітньо-наукова)
Освітня програма «Безпека державних інформаційних ресурсів»
(повна назва освітньої програми)

Керівник доц. Федюшин О.І.
(посада. прізвище, ініціали)

Допускається до захисту

Зав. кафедри _____ Халімов Г.З.
(підпис) (прізвище, ініціали)

2019 р.

Харківський національний університет радіоелектроніки

Факультет_____Комп'ютерної інженерії та управління_____
(повна назва)

Кафедра _____Безпеки інформаційних технологій _____
(повна назва)

Рівень вищої освіти_____другий (магістерський)_____

Спеціальність_____125 Кібербезпека_____
(код і повна назва)

Тип програми _____освітньо-професійна_____
(освітньо-професійна, або освітньо-наукова)

Освітня програма_____«Безпека державних інформаційних ресурсів»_____
(повна назва)

ЗАТВЕРДЖУЮ:
Зав. кафедри _____
(підпис)
«____»_____ 20 ___ р.

ЗАВДАННЯ
НА АТЕСТАЦІЙНУ РОБОТУ

студентові___Гавриленко Андрію Сергійовичу_____
(прізвище, ім'я, по батькові)

1. Тема роботи Аудит інформаційної безпеки в комп'ютерних мережах на базі Mikrotik
затверджена наказом по університету від 04 листопада 2019 р. № 1648Ст

2. Термін подання студентом роботи до екзаменаційної комісії 16 грудня 2019 р.

3. Вхідні дані до роботи Теоретичні відомості щодо механізмів захисту інформації в комп'ютерних мережах; технічна документація щодо особливостей експлуатації та використання мережного обладнання фірми Mikrotik; літературні джерела щодо використання засобів активного аудиту інформаційної безпеки в комп'ютерних мережах.

4. Перелік питань, що потрібно опрацювати в роботі
1. Провести аналіз існуючих методів захисту в комп'ютерних мережах;
2. Розглянути та проаналізувати технічні рішення щодо безпечного функціонування обладнання Mikrotik в різних сегментах мережі;
3. Розробити політику безпеки та рекомендації для базового налаштування мережного обладнання Mikrotik;
4. Провести аудит налаштованої комп'ютерної мережі, зробити висновки.

5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій (п.5. включається до завдання за рішенням випускової кафедри)
Презентаційний матеріал у вигляді слайдів

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Терміни виконання етапів роботи	Примітка
1	Отримання завдання	02.09.19	виконано
2	Аналіз літературних джерел за темою атестаційної роботи	03.09.19-20.09.19	виконано
3	Аналіз технічних рішень щодо безпечного функціонування обладнання Mikrotik в різних сегментах мережі	21.09.19-22.10.19	виконано
4	Розробка політики безпеки та рекомендацій для базового налаштування мережного обладнання Mikrotik	23.10.19-18.11.19	виконано
5	Проведення аудиту інформаційної безпеки мережі	19.11.19-01.12.19	виконано
6	Оформлення пояснювальної записки та матеріалів презентації	02.12.19-14.12.19	виконано
7	Представлення роботи до захисту	16.12.2019	виконано

Дата видачі завдання _____ _____20__ р.

Студент _____
(підпис)

Керівник роботи _____ доц. Федюшин О.І.
(підпис) (посада, прізвище, ініціали)

РЕФЕРАТ

Атестаційна робота містить 109 с., 3 табл., 39 рис., 14 джерел.

КОМП’ЮТЕРНІ МЕРЕЖІ, ЗАХИСТ ІНФОРМАЦІЇ, MIKROTIK, ROUTER OS, FIREWALL, АУДИТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ МЕРЕЖІ.

Об'єкт дослідження – локальна комп`ютерна мережа на основі маршрутизатора Mikrotik, що підключена до мережі Інтернет.

Предмет дослідження – аудит інформаційної безпеки в комп’ютерних мережах на базі Mikrotik.

Мета роботи – розглянути ключові аспекти безпеки в комп’ютерних мережах, побудованих на основі обладнання Mikrotik.

Основним завданням роботи є виявлення вразливостей обладнання Mikrotik за допомогою методів активного аудиту.

В роботі запропонована модель політики безпеки та рекомендації для базового налаштування мережного обладнання Mikrotik. Проведено експериментальні дослідження запропонованої конфігурації засобами пентестування.

Запропонований оптимальний варіант мережевого обладнання для рівня малого та середнього бізнесу.

ABSTRACT

The appraisal work contains 109 pages, 3 tables, 39 figures, 14 sources.

COMPUTER NETWORKS, PROTECTION OF INFORMATION, MIKROTIK, ROUTER OS, FIREWALL, NETWORK SECURITY AUDIT.

The object of study is a local computer network based on the Mikrotik router connected to the Internet.

The subject of the study is an audit of information security on Mikrotik-based computer networks.

Purpose - is to consider key security aspects of computer networks built on Mikrotik equipment.

The paper offers a security policy model and recommendations for basic setup of Mikrotik network equipment. Experimental studies of the proposed configuration by means of pentesting instruments have been carried out.

The optimal variant of the network equipment for the level of small and medium business is offered.

ЗМІСТ

УМОВНІ ПОЗНАЧЕННЯ

КІС – Комп’ютерна інформаційна система

ІС – Інформаційна система

КМ – Комп’ютерна мережа

КМО – Комп’ютерна мережа організації

ІБ – Інформаційна безпека

ОС – Операційна система

ПЗ – Програмне забезпечення

НСД – Несанкціонований доступ

СЗІБ – Система забезпечення інформаційної безпеки

ЦП – Центральний процесор

DNS – Domain Name System

FTP – File Transport Protocol

IDS – Intrusion Detection System

IIS – Internet Information Services

SSH – Secure Shell

SSL – Secure Socket Layer

VPN – Virtual Private Network

REP – Robots Exclusion Standard

SSI – Server Side Includes

ASP – Active Server Pages

ISP – Internet Service Provider

ВСТУП

На даний момент неможливо уявити роботу малого бізнесу без використання комп’ютерних технологій. Частіше за все необхідно будувати локальні або корпоративні мережі, в яких зазвичай задіяні майже всі комп'ютери компанії. Однак з моменту появи мереж виникла проблема безпеки. Багато керівників бізнесу навіть не замислюються над тим, як несанкціонований вхід у корпоративну мережу може вплинути на роботу організації.

Кожен керівник повинен розуміти важливість захисту своєї мережі від несанкціонованих втручань в роботу системи з глобальної, локальної мережі тощо. Кожна поважаюча себе компанія спілкується з іншими локальними мережами через Інтернет, оскільки встановити окремі канали зв'язку між окремими філіями досить дорого, а дозволити собі це можуть лише найбільші компанії. Як результат, можна очікувати порушення захисту мережі не лише від співробітників їхньої компанії, але і від хакерів через Інтернет та збоку конкуруючих компаній, які можуть наймати тих самих хакерів і направити їх діяльність на завдання матеріальної шкоди компанії шляхом виходу із строю якихось зовнішніх чи внутрішніх ресурсів, або викрадення інформації, що являється комерційною таємницею.

1 АНАЛІЗ ПРОБЛЕМ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Під загрозою безпеки вважається можлива небезпека (потенційна чи реальна), здійснення будь-якої дії (дії чи бездіяльності), спрямованої проти об'єкта захисту (інформаційних ресурсів), що завдає шкоди власнику чи користувачеві, проявляється як небезпека спотворення, розголошення або втрати інформації.

Реалізація загрози безпеці може переслідувати наступні цілі:

- Порушення конфіденційності інформації. Інформація, що зберігається та обробляється в комп'ютерній мережі організації (КМО), може бути дуже корисною для власника. Її використання сторонніми особами завдає значної шкоди інтересам власника;
- Порушення цілісності інформації. Втрата цілісності інформації (повна або часткова, компромісна, дезінформаційна) є загрозою, близькою до їх розголошення. Цінна інформація може бути втрачена або змінена шляхом несанкціонованого видалення або модифікації. Збиток, заподіяний такими діями, може бути набагато більшим, ніж при порушенні конфіденційності;
- Порушення (часткове або повне) працездатності КМО (порушення доступності). Зміна або неналежна модифікація режимів роботи компонентів КМО, їх модифікація або заміна можуть призвести до невірних результатів, відмови КМО від інформаційного потоку або відмови в обслуговуванні. Відмова від обігу інформації означає невпізнання однією із сторін взаємодії факту передачі чи прийому інформації. За умови, що ці повідомлення можуть містити звіти, розпорядження, важливі фінансові схвалення тощо, шкода в цьому випадку може бути дуже суттєвою.

Тому забезпечення інформаційної безпеки комп'ютерних систем та мереж є одним із головних напрямків розвитку інформаційних технологій.

Інформаційна система підприємства (мережа) - інформаційна система, учасниками якої може бути обмежене коло людей, визначена її власником або за згодою учасників цієї інформаційної системи (із закону про цифровий підпис).

Комп'ютерні мережі організації (КМО) - це розподілені комп'ютерні системи, що забезпечують автоматизовану обробку інформації. Проблема інформаційної безпеки лежить в основі цих комп'ютерних систем. Забезпечення безпеки КМО передбачає організацію боротьби проти будь-якого несанкціонованого вторгнення в операційний процес КМО, а також спроби модифікувати, вкрасти, дезактивувати або знищити його компоненти, тобто захистити всі компоненти комп'ютерної мережі - обладнання, програмне забезпечення, дані та персонал.

Подивимося, як наразі стоїть питання інформаційної безпеки в компаніях.

Дослідницька компанія Gartner Group визначає 4 рівні зрілості бізнесу з точки зору інформаційної безпеки (IS):

1) Рівень 0:

- в компанії ніхто не займається інформаційною безпекою (ІБ), керівництво компанії не усвідомлює важливості проблем ІБ;
- відсутність фінансування;
- ІБ реалізується за допомогою стандартних інструментів операційної системи, СУБД та додатків (захист паролем, контроль доступу до ресурсів та послуг).

Найбільш відповідний приклад тут - фірма з невеликим персоналом, яка займається, наприклад, купівлею чи продажем товарів. Всі технічні проблеми покладаються на адміністратора мережі, який доволі часто є студентом, адже студенту не треба багато платити. Суть тут полягає в тому, щоб все працювало, і нікого не бентежать можливі проблемі несанкціонованого втручання.

2) Рівень 1:

- ІБ розглядається керівництвом як суто "технічна" проблема, не існує єдиної програми (концепції, політики) для розвитку системи інформаційної безпеки компанії (ISMS);
- Фінансування здійснюється в рамках загального бюджету IT;

- ІБ реалізується за допомогою інструментів резервного копіювання, антивірусного ПЗ, брандмауерів, засобів організації VPN (традиційні засоби захисту).

3) 2 і 3 рівні:

- ІБ розглядається керівництвом як сукупність організаційно-технічних заходів, є розуміння важливості ІБ для виробничих процесів, є програма розвитку SGSI, затверджена компанією;
- фінансування передбачено в окремому бюджеті;
- ІБ реалізується за допомогою першого рівня + засобів поліпшеної аутентифікації, засобів аналізу електронних повідомлень та веб-контенту, IDS/IPS (системи виявлення вторгнень), інструментів аналізу безпеки, SSO (унікальні методи аутентифікації), PKI (інфраструктура відкритих ключів) та організаційні заходи (внутрішній та зовнішній) аудит, аналіз ризиків, політика інформаційної безпеки, положення, процедури, положення та директиви).

Відмінності 3-го рівня від 2-го:

- ІБ є частиною корпоративної культури, яку призначає CISA (Старший співробітник інформаційної безпеки);
- фінансування здійснюється в рамках окремого бюджету, який, за результатами досліджень аналітичної компанії Datamonitor, у більшості випадків не становить більше 5% IT-бюджету;
- ІБ реалізується за допомогою систем управління другого рівня + СУІБ, SOC (відділ реагування на загрози кібербезпеки).

Таким чином, серйозний підхід до питань ІБ з'являється лише на 2-му та 3-му рівнях. А на 1-му та частково 0-му рівні зрілості, згідно з цією класифікацією, існує так званий «фрагментований» підхід щодо забезпечення безпеки інформації. "Роздроблений" підхід має на меті протистояти чітко визначеним загрозам у даному середовищі. В якості прикладів реалізації цього підходу можна назвати індивідуальні засоби контролю доступу, окремі засоби шифрування, спеціалізовані антивірусні програми тощо.

Перевагою такого підходу є його висока вибірковість перед конкретною загрозою. Основним недоліком такого підходу є відсутність єдиного безпечного середовища обробки інформації. Заходи щодо захисту фрагментованої інформації захищають лише конкретні об'єкти комп'ютерної мережі від конкретної загрози. Навіть невелика зміна загрози призводить до втрати ефективності захисту.

За статистикою Gartner, у 2016 році 80% цих компаній (0 - 25%, 1 - 55%).

Більш серйозні організації, що відповідають 2-му та 3-му рівню зрілості класифікації Gartner, застосовують "глобальний" підхід до забезпечення безпеки інформації. Такий же підхід пропонують і великі компанії, які професійно займаються інформаційною безпекою.

Комплексний підхід заснований на вирішенні набору проблем в окремій області системи. Цей підхід в даний час є ключовим для створення безпечного середовища обробки інформації в корпоративних системах, яке об'єднує різні заходи протидії загрозам. Сюди входять юридичні, моральні, етичні, організаційні, програмні та технічні методи забезпечення інформаційної безпеки. Комплексний підхід дозволяє інтегрувати декілька автономних систем, інтегруючи їх у інтегровані системи безпеки.

Методи вирішення проблем безпеки тісно пов'язані з рівнем розвитку науки і техніки, зокрема рівнем технологічного забезпечення. Характерною тенденцією розвитку сучасної технології є процес повної інтеграції. Ця тенденція охоплює мікроелектроніку та комунікаційні технології, сигнали та канали, системи та мережі. Приклади включають надзвичайно великі інтегральні схеми, інтегровані мережі передачі даних, багатофункціональні пристрої зв'язку тощо.

Сучасний розвиток інтегрованого підходу або його максимальної форми - це комплексний підхід, заснований на інтеграції різних підсистем безпеки та підсистем зв'язку в єдину інтегровану систему із загальними технічними засобами, каналами зв'язку, програмним забезпеченням та базами даних. Комплексний підхід спрямований на забезпечення інтегрованої безпеки. Основним змістом концепції інтегрованої безпеки є необхідність забезпечення такого стану роботи компанії, при якому вона надійно захищена від усіх видів

можливих загроз протягом усього безперервного виробничого процесу. Поняття інтегрованої безпеки передбачає обов'язкову безперервність процесу захисту, протягом усього циклу технологічної діяльності з обов'язковим урахуванням усіх видів можливих загроз (несанкціонований доступ, видалення інформації, тероризм, пожежа, стихійні лиха т.п.).

Незалежно від форми інтегрованого або комплексного підходу, він завжди спрямований на вирішення ряду конкретних проблем у їх тісному взаємозв'язку за допомогою загальних технічних засобів, каналів зв'язку та програмного забезпечення. Наприклад, стосовно інформаційної безпеки найбільш очевидними завданнями є обмеження доступу до інформації, технічне та криптографічне закриття інформації, обмеження рівнів електромагнітних викидів технічного обладнання, охорона та сигналізація. Однак потрібно вирішувати й інші, не менш важливі завдання. Наприклад, недієздатність керівників бізнесу, членів сім'ї або ключових працівників може поставити під сумнів саме існування бізнесу. Стихійні лиха, аварії, тероризм тощо. Як результат, тільки інтегровані системи безпеки, які байдужі до типу загрози безпеці та забезпечують необхідний захист на постійній основі, можуть об'єктивно гарантувати повну безпеку інформації в ході процесу підготовки, обробки, передачі та зберігання інформації.

2 АНАЛІЗ ЗАГРОЗ МЕРЕЖЕВОЇ БЕЗПЕКИ

Набір протоколів TCP/IP використовується для організації зв'язку в неоднорідному мережевому середовищі, забезпечуючи сумісність між комп'ютерами різних типів. Сумісність є однією з головних переваг TCP/IP, тому більшість комп'ютерних мереж підтримують ці протоколи. Крім того, TCP/IP забезпечує доступ до глобальних Інтернет-ресурсів.

Через свою популярність TCP/IP став фактичним стандартом для взаємодії. Однак повсюдність стеку протоколів TCP/IP виявила його слабкі сторони. Створюючи свою оригінальну ідею, архітектори стеку TCP/IP не бачили причин турбуватися про захист мереж, побудованих на цій основі. Тому технічні характеристики більш ранніх версій протоколу IP не містили вимог безпеки, що призвело до початкової вразливості реалізації цього протоколу.

2.1 Питання безпеки IP-мережі

Зростаюча популярність Інтернет-технологій супроводжується зростанням серйозних загроз розкриття персональних даних, основних бізнес-ресурсів, державної таємниці тощо. Хакери та інші кіберзлочинці загрожують інформаційним ресурсам мережі з метою доступу до них за допомогою спеціальних атак. Ці напади стають більш складними в плані удару і не ускладнюються у виконанні. Цьому сприяють два основні фактори.

Перший - це широке проникнення Інтернету. Друге, це розповсюдження простих і зручних ОС та середовищ розробки. Цей фактор суттєво знижує рівень вимог до знань порушника. Раніше зловмиснику потрібні були високі навички програмування для створення та розповсюдження зловмисних програм. Зараз, щоб отримати доступ до інструменту хакера, вам просто потрібно знати потрібний сайт, де можно завантажити вже готові експлойти, а для успішної атаки потрібно просто натиснути на кнопку «зламати».

Проблеми інформаційної безпеки в корпоративних комп’ютерних мережах спричинені загрозою безпеці місцевих робочих станцій, локальних мереж та нападами на корпоративні мережі, що мають доступ до мереж передачі даних.

Мережеві атаки настільки ж різноманітні, як і системи, проти яких вони спрямовані. Деякі атаки дуже складні, інші може проводити звичайний оператор, навіть не знаючи, якими будуть наслідки його діяльності.

Розглянемо яку мету може мати нападник:

- порушення конфіденційності інформації, що передається;
- порушення цілісності та достовірності інформації, що передається;
- порушення працездатності всієї системи або окремих її частин.

Розподілені системи в основному сприйнятливі до віддалених атак, оскільки компоненти розподілених систем зазвичай використовують відкриті канали передачі даних, і зловмисник може не тільки пасивно прослуховувати інформацію, що передається, але й змінювати цю інформацію, і якщо на активний вплив на трафік можна виправити, то пасивний ефект практично не виявляється. Але оскільки під час роботи розподілених систем обмін службовою інформацією між компонентами системи також здійснюється відкритими каналами передачі даних, службова інформація стає тим самим об'єктом атаки, що і дані користувача.

Складність виявлення факту проведення віддаленої атаки ставить цей вид протиправних дій на перше місце з точки зору небезпеки та перешкоджає швидкому реагуванню на загрозу, за підсумком злочинець швидше досягає успіху в нападі.

Захищеність локальної мережі відрізняється від безпеки взаємодії з зовнішніми мережами тим, що в першу чергу виконуються несанкціоновані дії з внутрішньої мережі, оскільки в цьому випадку канали передачі даних локальної мережі розташовані в контрольованій зоні, а їх виявлення і захист реалізується адміністративними методами.

2.1.1 Найбільш поширені напади

1) Прослуховування, або сніфінг. В основному дані в комп'ютерних мережах передаються в незахищеному форматі, що дозволяє зловмиснику, який мав доступ до ліній даних мережі, прослуховувати трафік. Для прослуховування в комп'ютерних мережах використовують спеціальну програму, тобто «сніфер». Сніфер пакетів - це прикладна програма, яка перехоплює всі мережеві пакети, передані в певній зоні.

Загрози прослуховування пакетів можна уникнути, використовуючи одноразові паролі для аутентифікації, встановлення апаратного та програмного забезпечення, що розпізнає прослуховування, та використання криптографічного захисту каналів зв'язку.

2) Модифікація даних. Зловмисник, який може прочитати ваші дані, зможе перейти до наступного кроку - редагувати їх. Дані пакету можуть бути змінені, навіть якщо зловмисник нічого не знає про відправника або одержувача.

3) Аналіз мережевого трафіку. Мета таких атак - прослуховування каналів зв'язку, аналіз переданих даних та службової інформації для вивчення топології та архітектури системи, отримання критичної інформації про користувача (наприклад, паролі або номери кредитних карт, що передаються в незашифрованій формі). Атакам цього типу піддаються такі протоколи, як FTP та Telnet, особливістю яких є те, що ім'я користувача та пароль передаються без додаткового шифрування, тобто у відкритому вигляді.

4) Заміна довіреної особи. Більшість мереж та операційних систем використовують IP-адресу комп’ютера, щоб визначити, чи є цей хост необхідним пунктом призначення. У деяких випадках можливе неправильне призначення IP-адреси (підміна IP-адреси відправника іншою адресою). Цей тип атаки називається підробкою IP.

Підробка IP-адреси відбувається, коли зловмисник всередині компанії або поза нею представляє себе законним користувачем. Він може використовувати IP-адресу, включену в діапазон дозволених IP-адрес, або авторизовану зовнішню

адресу, дозволену для доступу до певних інформаційних ресурсів. Зловмисник також може використовувати спеціальні програми, які формують IP-пакети таким чином, щоб вони виглядали як вихідні повідомлення з авторизованих внутрішніх адрес корпоративної мережі.

Слід пам’ятати, що підробку IP можна робити за умови автентифікації користувачів на основі IP-адрес, щоб уникнути атак підробки IP-адреси, необхідно ввести додаткові методи аутентифікації користувача (засновані на разових паролях або інших криптографічних методах).

5) Посередництво. Ця атака передбачає активне прослуховування, перехоплення та контроль даних, що передаються невидимим проміжним вузлом. Коли комп'ютери взаємодіють на низьких мережевих рівнях, вони не завжди можуть визначити, з ким вони обмінюються даними.

6) Посередництво в незашифрованому обміні ключами (атака "людина по середині"). Щоб здійснити атаку "людина посередині", зловмисник повинен мати доступ до пакетів, що передаються по мережі. Для атак такого типу часто використовуються пакетні сніфери, транспортні протоколи та протоколи маршрутизації.

Атаки «людина посередині» здійснюються для крадіжки інформації, перехоплення поточного сеансу та доступу до приватних ресурсів мережі, аналізу трафіку та отримання інформації про мережу та її користувачів, проведення DoS-атак, спотворення даних та передачі несанкціонованої інформації мережевим сесіям.

Ефективно боротися з атаками, такими як «людина посередині», можливо лише за допомогою криптографії.

7) Викрадення сесії. Після закінчення початкової процедури автентифікації з'єднання, встановлене законним користувачем, наприклад, з поштовим сервером, зловмисником перемикається на новий хост, і на вихідний сервер поступає команда відключитися. В результаті "співрозмовник" законного користувача непомітно замінюється.

8) Відмова в обслуговуванні (DoS). Ця атака відрізняється від інших типів атак: вона не призначена для несанкціонованого доступу до мережі або отримання інформації з цієї мережі. DoS-атаки роблять мережу організації недоступною для звичайного використання шляхом перевищення дозволених лімітів мережі, операційної системи чи програми. По суті, вони не дають змоги користувачам мережі отримати доступ до ресурсів або комп'ютерів організації.

DoS може використовувати загальні протоколи Інтернету, такі як TCP або ICMP.

9) Напади на паролі. Їх мета - визначити пароль та ім’я користувача законного користувача. Зловмисники можуть проводити атаки на паролі, використовуючи наступні методи:

- підробка IP-адреси;
- прослуховування (сніфінг);
- простий перебор паролей (brute force).

Атаки на паролі можна уникнути, якщо ви не використовуєте текстові паролі. Використання одноразових паролів та криптографічної аутентифікації може практично усунути загрозу таких атак. На жаль, не всі програми, хости та пристрої підтримують ці методи аутентифікації.

10) Атаки на рівні додатків.

Атаки на рівні додатків можуть бути виконані декількома способами, найбільш поширеним є використання відомих недоліків серверного програмного забезпечення (FTP, HTTP, веб-сервер). Основна проблема при атаках на рівні додатків полягає в тому, що вони часто використовують порти, яким дозволено перетинати міжмережевий екран. Інформація про атаки на рівні додатків широко публікується, щоб допомогти адміністраторам вирішити проблему за допомогою модулів виправлення (патчів).

Повністю усунути атаки на рівні програми неможливо. Хакери постійно виявляють і публікують на своїх веб-сайтах нові вразливості.

Тут важливе гарне адміністрування системи. Щоб зменшити вразливість до таких атак, можна вжити наступні кроки:

- Проаналізувати файли журналів операційної системи та журналів міжмережевих фільтрів;
- Слідкувати за даними CERT (комп'ютерна група реагування на надзвичайні події) про слабкі сторони програм, операційних систен, нових виявлених вразливостях;
- використовувати останні версії операційної системи, додатків та останні виправлення;
- використовувати системи розпізнавання атак IDS/IPS.

11) Мережева розвідка - це збір інформації в мережі з використанням загальнодоступних даних та програм. Готуючи атаку на будь-яку мережу, зловмисник зазвичай намагається отримати якомога більше інформації про неї.

Мережева розвідка проводиться у вигляді запитів DNS, ping-запитів та сканування портів. Запити DNS допоможуть зрозуміти, хто є власником певного домену та які адреси призначені цьому домену. Тестування адреси за допомогою DNS, дозволяють побачити, які хости фактично працюють у даному середовищі. Отримавши список хостів, зловмисник використовує інструменти аналізу портів для складання повного списку служб, підтримуваних цими хостами. В результаті отримується інформація, яка ймовірно може бути використана для злому.

Системи IDS/IPS мережевого та рівня хоста зазвичай добре допомагають інформувати адміністратора про відкриття мережі, що допомагає вчасно повідомити адміністратора про порушення та краще підготуватися до можливої наступної атаки.

12) Комп'ютерні віруси, мережеві «черв’яки», програма «троянський кінь».

Віруси - це зловмисні програми, які втручаються в інші програми для виконання деякої небажаної функції на робочій станції кінцевого користувача.

Варіант вірусної програми - мережевий черв'як, який поширюється по всій глобальній мережі і не залишає своєї копії на носіях інформації. Щоб убезпечити себе від «черв’яка», потрібно вжити заходів щодо несанкціонованого доступу до внутрішньої мережі.

До комп'ютерних вірусів примикають так звані «трояни». "Троянський кінь" - це програма, яка виглядає як корисна програма, але насправді вона виконує шкідливі функції (знищуючи програмне забезпечення, копіюючи та надсилаючи файли, що містять дані, чутливі до зловмисника тощо). [2]

Щоб захистити себе від цих шкідливих програм, потрібно:

- виключення несанкціонованого доступу до виконуваних файлів;
- тестування придбаного програмного забезпечення;
- перевірка цілісності виконуваних файлів та системних областей;
- створити закрите середовище для виконання програми.

Атаки, перелічені в мережах IP, можливі через:

- використання публічних каналів передачі даних. Найважливіші дані, можуть передаватись по мережі в незашифрованому вигляді;
- вразливості в процедурах аутентифікації;
- інформація про особу на рівні IP передається відкритим текстом;
- відсутність у базовій версії стека протоколу TCP/IP механізмів, що гарантують конфіденційність та цілісність переданих повідомлень;
- аутентифікація відправника за IP-адресою. Процедура аутентифікації проводиться лише на етапі встановлення з'єднання, а надалі справжність отриманих пакетів не перевіряється;
- відсутність контролю над маршрутом повідомлень в Інтернеті, що робить віддалені атаки практично безкарними.

2.1.2 Загрози та вразливості провідних корпоративних мереж

На початковому етапі розвитку мережевих технологій збиток від вірусів та інших видів комп’ютерних атак був низьким, оскільки залежність світової економіки від інформаційних технологій була незначною. В даний час, в умовах сильної залежності компанії від електронних засобів доступу, обміну інформацією та постійно зростаючої кількості атак, шкода, заподіяна найбільш

незначними атаками може коштувати мільйонів доларів, а загальний річний збиток світовій економіці становить десятки мільярдів доларів.

Інформація, що обробляється в корпоративних мережах, є особливо вразливою, на це впливає:

- збільшення обсягу інформації, що обробляється, передається та зберігається в комп’ютерах;
- концентрація в базах даних інформації різного рівня важливості та конфіденційності;
- розширення доступу кола користувачів до інформації, що зберігається в базах даних та ресурсах комп'ютерної мережі;
- збільшення кількості віддалених робочих місць;
- широке використання глобального Інтернету та різних каналів зв'язку;
- автоматизація обміну інформацією між комп'ютерами користувачів.

Аналіз найбільш поширених загроз для сучасних провідних корпоративних мереж показує, що джерела загроз можуть варіюватися від несанкціонованих дій хакерів до комп'ютерних вірусів, прицому людські помилки є значним ризиком для інформаційної безпеки. Слід мати на увазі, що джерела загроз безпеці можуть знаходитися як всередині інформаційної системи, так і бути із зовнішніх джерел. Такий поділ виправданий тим, що для однакової загрози (наприклад, крадіжки) контрзаходи щодо зовнішніх та внутрішніх джерел різні. Знання можливих загроз, а також вразливостей інформаційної системи необхідне для вибору найбільш ефективних засобів забезпечення безпеки.

Найбільш поширені та небезпечні помилки (з точки зору шкоди) - це ненавмисні помилки користувачів, операторів та системних адміністраторів, які обслуговують КІС. Іноді ці помилки спричиняють прямий збиток (неправильно введені дані, програмна помилка, яка спричинила зупинку або збій системи), а іноді вони створюють слабкі місця, якими можуть скористатися зловмисники (зазвичай це помилки адміністративні).

За даними Національного інституту стандартів і технологій Сполучених Штатів (NIST), 55% порушень безпеки інформаційної системи є результатом

ненавмисних помилок. Робота в глобальній ІС робить цей фактор дуже актуальним, і джерелом шкоди можуть бути як дії користувачів організації, так і користувачів глобальної мережі, що є особливо небезпечним. На рис. 2.1 - кругова діаграма, що показує статистику джерел порушень безпеки в СНД.

На другому місці, з точки зору збитків, стоять крадіжки та підробки. У більшості розглянутих випадків винні особи були штатними працівниками організацій, які були знайомі з режимом роботи та захисними заходами. Наявність потужного інформаційного каналу для зв'язку з глобальними мережами за відсутності належного нагляду за його роботою може ще більше сприяти цій діяльності.

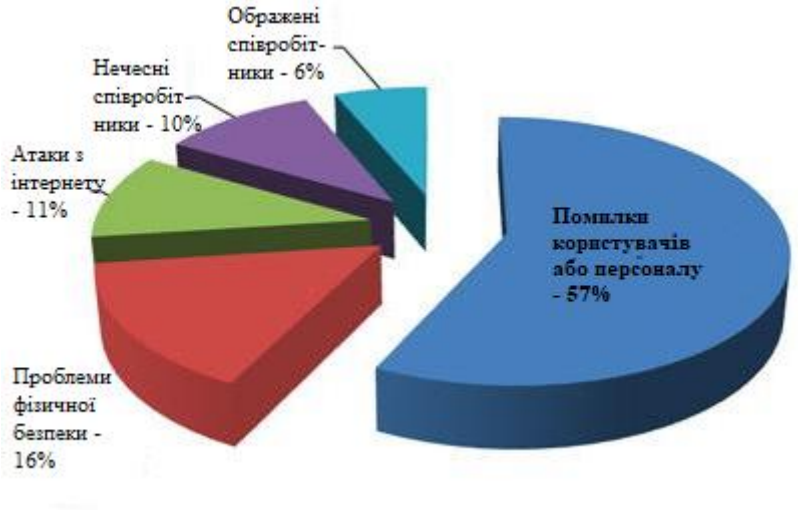

Рисунок 2.1 - Джерела порушень безпеки

Ображені працівники, навіть колишні працівники, знають порядок організації та здатні завдати шкоди дуже ефективно. Отже, у разі звільнення працівника його права доступу до інформаційних ресурсів повинні бути відкликані.

Навмисні спроби отримати несанкціонований доступ через зовнішні комунікації складає приблизно 10% усіх можливих порушень. Хоча ця величина і не здається такою великою, досвід показує, що майже всі інтернет-сервери атакуються кілька разів на день. Тести Агенції захисту інформаційних систем (США) показали, що 88% комп'ютерів мають слабкі сторони інформаційної безпеки, які можна активно використовувати для отримання несанкціонованого

доступу. Окремо слід розглянути випадки віддаленого доступу до інформаційних структур організацій.

Перш ніж будувати політику безпеки, необхідно оцінити ризики, яким піддається IT-середовище організації, та вжити відповідних заходів. Зрозуміло, що витрати на контроль та запобігання загрозам безпеки організації не повинні перевищувати очікуваних втрат.

Ця статистика може вказати адміністрації та персоналу організації, куди слід спрямовувати зусилля на ефективне зменшення загроз безпеці корпоративної мережі та системи. Звичайно, ви повинні керувати проблемами фізичної безпеки та вживати заходів для зменшення негативного впливу на безпеку людських помилок, але в той же час ви повинні приділяти максимум уваги вирішенню питань безпеки мережі, щоб запобігати атакам на корпоративну мережу та систему, ззовні та зсередини системи.

2.1.3 Загрози та вразливості бездротових мереж

Під час побудови бездротових мереж існує також проблема забезпечення їх безпеки. Якщо у звичайних мережах інформація передається дротом, радіохвилі, що використовуються для бездротових рішень, можуть бути легко перехоплені відповідним обладнанням. Принцип роботи бездротової мережі призводить до великої кількості можливих вразливих ситуацій для атак та проникнення.

Обладнання бездротової локальної мережі (WLAN) включає точки бездротового доступу та робочі станції для кожного абонента.

Точки доступу AP (точка доступу) виконують роль вузлів, що забезпечують зв'язок між абонентами та між собою, а також функцію мостів, які спілкуються з локальною провідною мережею та Інтернетом. Кожна точка доступу може обслуговувати декілька абонентів. Кілька сусідніх точок доступу утворюють зону доступу Wi-Fi, в межах якої всі абоненти, оснащені бездротовими адаптерами, мають доступ до мережі. Ці зони доступу створюються в переповнених місцях: в аеропортах, кампусах, бібліотеках, магазинах, бізнес-центрах тощо.

Основна відмінність провідних та бездротових мереж - наявність неконтрольованої області між кінцевими точками бездротової мережі. Це дозволяє зловмисникам, близьким до бездротових структур, розпочати серію атак, неможливих у провідному світі.

Під час використання бездротової локальної мережі ризики безпеки значно зростають (рис. 2.2).

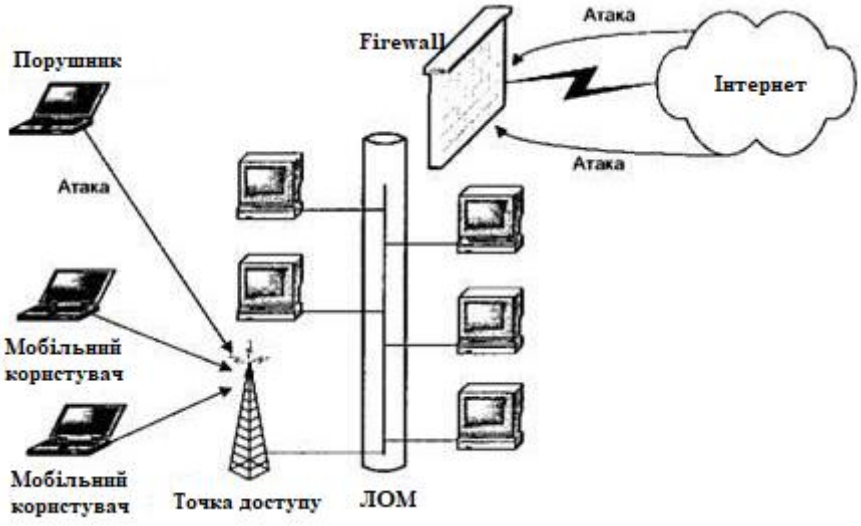

Рисунок 2.2 - Загрози з бездротовим доступом до локальної мережі

Ми перераховуємо основні вразливості та загрози бездротових мереж:

1) Трансляція радіомаяка. Точка доступу включає в себе радіомаяк з певною частотою для повідомлення бездротових вузлів поблизу о його присутності. Ці широкомовні сигнали містять основну інформацію про бездротову точку доступу, включаючи, як правило, SSID, і спонукають бездротові вузли до реєстрації в цій області. Будь-яка робоча станція в режимі очікування може отримати SSID та бути додана до відповідної мережі. Маякове мовлення - це "вроджена патологія" бездротових мереж. Багато моделей дозволяють деактивувати частину цієї трансляції, що містить SSID, щоб дещо ускладнити бездротове прослуховування, але SSID все-таки надсилається при підключенні, тому є невелике вікно вразливості.

2) Прослуховування. Прослуховування проводиться для збору інформації про мережу, яка повинна атакувати пізніше. Перехоплювач може використовувати

витягнуті дані для доступу до мережевих ресурсів. Обладнання, яке використовується для прослуховування в мережі, може бути не складнішим, ніж обладнання, яке використовується для звичайного доступу до цієї мережі. Бездротові мережі дозволяють за своєю природою підключати комп'ютери, розташовані на певній відстані від неї, до фізичної мережі, як ніби ці комп’ютери знаходяться безпосередньо в мережі. Наприклад, людина, яка сидить у припаркованому поблизу автомобілі, може підключитися до бездротової мережі в будівлі. Пасивну атаку прослуховування виявити майже неможливо.

3) Помилкові точки доступу до мережі. Досвідчений зловмисник може організувати підроблену точку доступу з імітаційними мережевими ресурсами. Не підозрюючи абонентів, вони звертаються до цієї підробленої точки доступу та передають їй важливі деталі, такі як інформація про автентифікацію. Цей тип атаки іноді використовується в поєднанні з прямим "заклинюванням" справжньої точки доступу до мережі.

4) Відмова в обслуговуванні. Повний параліч мережі може бути спричинений нападом DoS (відмовою в обслуговуванні). Його мета - перешкоджати доступу користувачів до мережевих ресурсів. Бездротові системи особливо сприйнятливі до таких атак. Фізичний рівень бездротової мережі - це абстрактний простір навколо точки доступу. Зловмисник може включити пристрій, який заповнює весь спектр на робочій частоті перешкодами та нелегальним трафіком - це завдання не становить великих труднощів. Факт фізичної атаки DoS у бездротовій мережі важко довести.

5) Людина посередині. Атаки такого типу здійснюються в бездротових мережах набагато легше, ніж у дротових мережах, оскільки у випадку з дротовою мережею потрібно реалізувати певний тип доступу до неї. Зазвичай напади середньої людини використовуються для руйнування конфіденційності та цілісності сеансу спілкування. MITM-атаки складніші, ніж більшість інших атак: вони вимагають детальної мережевої інформації. Зловмисник, як правило, підробляє особу одного з мережевих ресурсів. Він використовує можливість незаконного прослуховування та захоплення потоку даних для того, щоб змінити

його вміст, необхідний для задоволення деяких його цілей, наприклад, підроблення IP-адрес, зміни MAC-адреси для імітації іншого хоста тощо.

6) Анонімний доступ до Інтернету. Незабезпечені бездротові локальні мережі пропонують хакерам найкращий анонімний доступ для атак в Інтернеті. Хакери можуть використовувати незахищену бездротову локальну мережу організації для доступа в Інтернет, де вони будуть безслідно проводити незаконні дії. Організація з незахищеною локальною мережею офіційно стає джерелом трафіку атаки, орієнтованого на іншу комп'ютерну систему, що пов'язано з потенційним ризиком юридичної відповідальності за шкоду, заподіяну жертві нападу хакерами. [3]

Описані вище атаки є найпоширенішими, але це не єдині атаки, які використовуються хакерами для прориву в бездротові мережі.

3 МЕТОДИ ЗАХИСТУ КОМП'ЮТЕРНОЇ МЕРЕЖІ ОРГАНІЗАЦІЇ ВІД НСД ІЗ МЕРЕЖІ ІНТЕРНЕТ

Існує кілька підходів до вирішення проблеми захисту КМО, підключених до Інтернету, від несанкціонованого доступу. Перший підхід полягає в посиленні захисту всіх систем, доступних через Інтернет. Такий підхід називається «безпекою на рівні хоста». Це може включати навчання користувачів та системних адміністраторів роботі в більш ворожій обстановці, посилення політики захисту паролів (введення або застосування обмежень щодо мінімальної довжини, структури символів та строку дії пароля) або впровадження методів аутентифікації без пароля, посилення правил доступу до системи, посилення вимог використовуваного програмного забезпечення, включаючи операційні системи, і регулярна перевірка відповідності всіх впроваджених вимог.

Цей підхід має ряд недоліків:

- робочі процедури в системі для користувачів ускладнені, і, можливо, певні дії, до яких вони звикли, наразі заборонені. Це може призвести до зниження продуктивності користувачів, а також до незадоволення.
- системні адміністратори несуть дуже велике додаткове навантаження на підтримку системи. Навіть для відносно невеликих систем, що містять кілька десятків машин, завдання збереження заданого рівня безпеки може вимагати непропорційних зусиль.
- вимоги до захисту можуть суперечити вимогам щодо використання системи, і одна з них повинна віддавати перевагу на шкоду іншим. Загалом, вимоги до функціональності системи зазвичай стоять вище, ніж вимоги безпеки.

Перевага такого підходу полягає в тому, що, крім проблеми захисту від «зовнішнього ворога», він вирішує і проблему внутрішньої безпеки системи. Оскільки велика частка випадків порушення безпеки (за деякими даними, до 80%) походить від працівників або колишніх співробітників компаній, такий підхід може дуже ефективно підвищити загальну безпеку системи.

Другий підхід є найбільш радикальним. У цьому документі корпоративна мережа роботи фізично не підключена до Інтернету. Для взаємодії з Інтернетом використовуються одна або кілька спеціально виділених машин, які не містять конфіденційної інформації. Переваги такого підходу очевидні: оскільки операційна мережа не підключена до Інтернету, загроза несанкціонованого доступу з Інтернету в принципі відсутня. У той же час такий підхід має певні обмеження та недоліки. Обмеження в деяких випадках є прийнятним, це відсутність доступу до Інтернету з робочого місця працівників. Недоліки такого підходу полягають у наявності незахищених систем, підключених до Інтернету, які можуть бути предметом атаки «відмова в обслуговуванні» та крадіжках послуг (у тому числі тих, які можуть бути використані для злому інших систем). Варіантом такого підходу є розділення по протоколам. Наприклад, стек протоколів IPX/SPX використовується для доступу до корпоративних інформаційних ресурсів, а TCP/IP використовується для доступу до Інтернету. У той же час, наприклад, сервери будуть невидимі для хакера і не можуть бути атаковані безпосередньо з Інтернету. Цей підхід також має певні обмеження. Наприклад, це неприпустимо для мережі, де для доступу до внутрішніх ресурсів потрібен TCP/IP. Другий його недолік полягає в тому, що користувацькі системи є видимими та доступними з Інтернету і можуть використовуватися як основа для атак на сервера.

Третій підхід, який називається "безпека мережевого рівня", передбачає введення засобів обмеження доступу до точки мережевого з'єднання. Такий підхід дозволяє зосередити захист і управління в точках підключення двох або більше мереж, наприклад, в точці з'єднання КМО з Інтернетом. На даний момент існує спеціально виділена система - брандмауер, яка контролює обмін інформацією між двома мережами і фільтрує інформацію відповідно до визначених правил, визначених політикою безпеки компанії. Усі обміни даними між Інтернетом та внутрішньою мережею проходять через брандмауер. Організація може значно виграти від цієї моделі безпеки. Єдина система, яка виконує функції брандмауера, може захистити десятки і сотні систем, що стоять за нею, від несанкціонованого

доступу без встановлення до них додаткових вимог безпеки. Перевагами цього підходу є концентрація захисту та контролю в даний момент часу, мінімальна модифікація внутрішніх процедур, що дозволяють користувачам працювати з інформаційною системою, порівняно велика простота управління та можливо вищий рівень захисту. Обмеженням цього підходу є те, що він призначений лише для захисту від зовнішніх загроз від віддалених спроб атаки.

Зараз ми розглянемо типову КМО з точки зору застосовності вищезазначених методів захисту. Як правило, це клієнтські комп'ютери, на яких працює Microsoft Windows 10 або рідше Windows 7 або 8, сервери з операційною системою Microsoft Windows Server, Novell Netware та/або різні системи Unix або інше мережеве обладнання, наприклад мережеві принтери, концентратори, комутатори та маршрутизатори з можливістю дистанційного керування тощо.

У цьому випадку використання моделі безпеки виключно на хостовому рівні може бути неприйнятним через велику складність (і, можливо, практичну неможливість реалізації) доведення рівня безпеки систем, які використовуються для необхідного рівня. Якщо використання системи, фізично відокремленої від основної мережі для доступу до Інтернету, є неприйнятною, найефективнішим рішенням є використання технології брандмауера.

Брандмауер - це локальний (монокомпонентний) або функціонально розподілений інструмент, який реалізує керування інформацією, що надходить до автоматизованої системи та/або залишає автоматизовану систему, і захищає автоматизовану систему шляхом фільтрації інформації, тобто його аналіз на основі набору критеріїв та рішення про розповсюдження його в (або з) автоматизованій системі. При правильному використанні брандмауери - це дуже ефективний засіб захисту від загроз корпоративним мережам з Інтернету.

3.1 Теоретичні питання побудови міжмережевих екранів

3.1.1 Архітектура брандмауера

Брандмауери можуть бути налаштовані як одна з декількох архітектур, які пропонують різний рівень безпеки при різних витратах на встановлення та обслуговування. Організації повинні проаналізувати свій профіль ризику та вибрати відповідну архітектуру. Нижче наведені типові архітектури брандмауера та приклади політики безпеки для них.

Існують брандмауери з такими архітектурами:

1) Хост, підключений до двох мережевих сегментів

Це хост, який має декілька мережевих інтерфейсів, і кожен інтерфейс до мережі фізично з'єднаний з окремим мережевим сегментом. Найпоширеніший приклад - хост, підключений до двох сегментів.

Брандмауер на основі хоста, підключений до двох мережевих сегментів, - це брандмауер з двома мережевими адаптерами, кожен з яких підключений до окремої мережі. Наприклад, одна мережева карта підключена до зовнішньої або незахищеної мережі, а інша - до внутрішньої або захищеної мережі. У цій конфігурації ключовим принципом безпеки є заборона прямої маршрутизації трафіку від ненадійної мережі до надійної мережі - брандмауер завжди повинен бути проміжною ланкою.

Маршрутизація повинна бути відключена на такому брандмауері, щоб IP-пакети з однієї мережі не змогли переходити до іншої мережі.

Ця конфігурація, мабуть, одна з найдешевших і найпоширеніших, коли організація має віддалене підключення локальної мережі до Інтернету. Цим займається машина, на якій встановлено FreeBSD, і маршрутизація на ній заборонена, крім того, фільтр пакетів (ipfw), інтегрований в ядро, налаштований відповідно.

2) Екранований хост

Для такої архітектури, як екранований хост, використовується хост (який називається хостом-бастіону), з яким може з'єднуватися будь-який зовнішній

хост, але доступ до всіх інших менш захищених внутрішніх хостів заборонено. Для цього маршрутизатор фільтра налаштований так, що всі з'єднання із внутрішньою мережею із зовнішніх мереж перенаправляються до хоста-бастіону.

Якщо встановлено шлюз фільтрації пакетів, хост-бастіон повинен бути налаштований так, щоб всі з'єднання із зовнішніх мереж проходили через нього, щоб запобігти прямому зв’язку між комп'ютерною мережею організації та Інтернетом.

3) Екранова підмережа

Архітектура екранованої мережі по суті збігається з архітектурою екранованого хоста, але додає ще одну лінію захисту, створюючи мережу, в якій розташований хост-бастіон, окремо від внутрішньої мережі.

Екрановану підмережу необхідно реалізувати, додавши мережу периметру, щоб відокремити внутрішню мережу від зовнішньої. Це гарантує, що навіть у разі успішної атаки на бастіон-хост, зловмисник не зможе вийти за межі периметрової мережі через те, що між внутрішньою та домашньою мережею існує ще один захисний маршрутизатор.

3.1.2 Класифікація брандмауерів

Брандмауери - це пристрої або системи, які контролюють потік мережевого трафіку між мережами з різними вимогами безпеки. У більшості сучасних програм брандмауери та їх оточення обговорюються в контексті Інтернет-з'єднань і, отже, використання стека протоколів TCP / IP. Однак брандмауери також використовуються в мережевих середовищах, які не вимагають обов'язкового підключення до Інтернету. Наприклад, у багатьох корпоративних корпоративних мережах встановлено міжмережеві екрани для обмеження з'єднань із внутрішніми мережами та від них, які обробляють інформацію різного рівня чутливості, наприклад бухгалтерський облік чи інформацію про клієнтів. Визначаючи брандмауери для управління з'єднаннями з цими зонами, організація може запобігти несанкціонованому доступу до відповідних систем та ресурсів у

чутливих зонах. Таким чином, використання брандмауера забезпечує додатковий рівень безпеки, якого не можна було б досягти інакше.

В даний час існує кілька типів брандмауерів. Один із способів порівняння їх можливостей - це перелік рівнів моделі OSI, яку цей тип брандмауера може аналізувати. Модель OSI - це абстрагування мережевого зв'язку між комп'ютерними системами та мережевими пристроями. Розглянемо лише рівні моделі OSI, пов'язані з брандмауерами. На рисунку 3.1 показаний стек протоколу моделі OSI.

Сукупність протоколів, які забезпечують взаємодію двох систем і передачу повідомлень між ними, утворює *стек протоколів.*

Стеки мережних протоколів, які використовують найчастіше, їх порівняння із рівнями еталонної моделі OSI.

Рівні моделі OSI	IBM/ Microsoft	TCP/IP	Novell	Стек OSI
Прикладний	SMB	Telnet,FTP, SMTP, NNTP, HTTP, SNMP		X.400, X.500, VTP, FTAM
Представницький			NCP, SAP	Протокол подання OSI
Сеансовий	NetBIOS	TCP		Сеансовий протокол OSI
Транспортний		UDP	SPX	Транспортний протокол OSI
Мережний	—	IP, ICMP, RIP, OSPF	IPX, RIP, NLSP	IS-IS
Канальний	Ethernet (802.3), Token Ring (802.5), FDDI, SLIP, PPP, X.25, ATM, LAP-B, LAP-D			
Фізичний				

Рисунок 3.1 - Стек протоколу моделі OSI

Рівень 1 - це фактичне обладнання для фізичного з'єднання, наприклад, Ethernet.

Рівень 2 - це рівень, на якому мережевий трафік передається через локальну мережу (LAN). Це також перший рівень із можливістю адреси, з яким можна ідентифікувати одну машину. Адреси присвоюються мережевим інтерфейсам і називаються адресами MAC (Media Access Control). Адреса Ethernet, що належить до Ethernet-картки, є прикладом MAC-адреси рівня 2.

Рівень 3 - це рівень, відповідальний за забезпечення мережевого трафіку через WAN. Адреси 3 рівня в Інтернеті називаються IP-адресами; адреси зазвичай унікальні, але в деяких обставинах, наприклад, при перекладі мережевих адрес (NAT), можливо, різні фізичні системи мають однакову IP-адресу 3 рівня.

Рівень 4 - ідентифікує конкретну мережеву програму та сеанс; система може мати велику кількість сеансів 4 рівня з іншими операційними системами. Термінологія, пов'язана з сімейством протоколів TCP/IP, включає поняття портів, які можуть розглядатися як точки завершення сеансу: номер порту джерела визначає сеанс зв'язку у вихідній системі; номер порту призначення визначає сеанс зв'язку системи призначення. Верхні рівні (5, 6 і 7) представляють додатки та системи для кінцевих користувачів.

Брандмауери класифікуються на:

- Міжмережеві екрани з фільтрацією пакетів;
- Шлюзи сеансового рівня;
- Шлюзи прикладного рівня;
- Міжмережеві екрани експертного рівня.

Міжмережеві екрани з фільтрацією пакетів - це маршрутизатори або серверні програми, налаштовані на фільтрацію вхідних та вихідних пакетів. Тому такі екрани іноді називають фільтрами пакетів. Фільтрація виконується шляхом аналізу IP-адреси, джерела та приймача, а також портів вхідних пакетів TCP або UDP, та порівняння їх із налаштованою таблицею правил. Ці брандмауери прості у використанні, недорогі та мають мінімальний вплив на продуктивність комп'ютерної системи. Основним недоліком є їх вразливість до підробки IP-адрес. Крім того, їх важко налаштувати: їх установка вимагає знання мережі, транспортних та прикладних протоколів.

Шлюзи сесійного рівня контролюють дійсність сеансу. Вони відстежують зв’язок між авторизованим клієнтом та зовнішнім хостом (і навпаки), визначаючи, чи потрібний сеанс запиту. Під час фільтрації пакетів шлюз рівня сеансу базується на інформації, що міститься в заголовках пакетів рівня сеансу протокола TCP, тобто він працює на два рівні вище, ніж брандмауер з

фільтруванням пакетів. Крім того, ці системи зазвичай мають функцію трансляції мережевих адрес, яка маскує внутрішні IP-адреси, тим самим виключаючи підробку IP-адрес. Однак у таких брандмауерах немає контролю над вмістом пакетів, що генеруються різними службами. Для усунення цього недоліку використовуються шлюзи рівня програми.

Шлюзи прикладного рівня перевіряють вміст кожного пакету, що проходить через шлюз, і можуть фільтрувати певні типи команд або інформацію в призначених їм протоколах рівня додатків. Це більш просунутий і надійний тип брандмауера, який використовує проксі-сервери або агенти програми. Агенти готуються до конкретних Інтернет-сервісів (HTTP, FTP, Telnet тощо) і використовуються для перевірки мережевих пакетів на достовірність даних.

Шлюзи прикладного рівня знижують продуктивність системи завдяки перетворення в програмі-посередниці. Це непомітно під час роботи в Інтернеті при роботі на низькошвидкісних каналах, але це важливо при роботі у внутрішній мережі.

Брандмауери експертного рівня поєднують елементи з трьох описаних вище категорій. Як і брандмауери фільтрації пакетів, вони працюють на мережевому шарі моделі OSI, фільтруючи вхідні та вихідні пакети на основі перевірки IP-адрес та номерів портів. Брандмауери рівня експертів також виконують завдання шлюзів сеансового рівня, визначаючи, чи належать пакети до відповідного сеансу. Нарешті, брандмауэры на рівні експертів беруть на себе функції шлюзу прикладного рівня, оцінюючи вміст кожного пакету відповідно до політики безпеки, розробленої в конкретній організації.

Замість використання середнього програмного забезпечення, пов’язаного з додатком, брандмауери експертного рівня використовують спеціальні алгоритми розпізнавання та обробку даних на рівні додатків. За допомогою цих алгоритмів пакети порівнюються з відомими моделями даних, які теоретично повинні забезпечувати більш ефективну фільтрацію пакетів. Незалежно від архітектури, брандмауер може мати додаткові послуги. Ці послуги включають трансляцію мережевих адрес (NAT), підтримку протоколу конфігурації динамічного хоста

(DHCP) та шифрування, складання кінцевої точки шлюзу VPN та фільтрацію на рівні вмісту. застосування.

Багато сучасних брандмауерів можуть функціонувати як шлюзи VPN. Наприклад, організація може надсилати незашифрований мережевий трафік із системи за брандмауером до віддаленої системи за корпоративним шлюзом VPN; брандмауер шифрує трафік і перенаправляє його до віддаленого шлюзу VPN, який розшифровує його і пересилає до цільової системи. Більшість популярних сьогодні брандмауерів поєднують ці функції.

Багато брандмауерів також включають різні технології фільтрування активного вмісту. Цей механізм відрізняється від звичайної функції брандмауера тим, що брандмауер тепер також має можливість фільтрувати фактичні дані програми на рівні 7, що проходить через нього. Наприклад, цей механізм можна використовувати для пошуку вірусів у файлах, приєднаних до електронної пошти. Він також може бути використаний для фільтрації найнебезпечніших технологій активного вмісту в Інтернеті, таких як Java, JavaScript та ActiveX. Або його можна використовувати для фільтрації вмісту або по ключовим словам, щоб обмежити доступ до невідповідних сайтів чи доменів. Однак компонент фільтрації, вбудований у брандмауер, не слід розглядати як єдиний можливий механізм фільтрації вмісту; Можна використовувати подібні фільтри при використанні стискання, шифрування чи інших технологій. [1][6]

3.2 Віртуальні приватні мережі (VPN)

Для ефективного протидії мережевим атакам та забезпечення активного і безпечного використання відкритих мереж на підприємстві на початку 90-х років народилась і активно розвивається концепція побудови захищених віртуальних приватних мереж (VPN).

3.2.1 Концепція побудови безпечних віртуальних приватних мереж VPN

Концепція побудови захищених віртуальних приватних мереж VPN заснована на досить простій ідеї: якщо у глобальній мережі є два вузли, які хочуть обмінюватися інформацією, то для забезпечення конфіденційності та цілісності інформації, що передається через відкриті мережі, необхідно побудувати віртуальний тунель, доступ до якого повинен бути надзвичайно важким для всіх можливих активних та пасивних зовнішніх спостерігачів. Термін "віртуальний" означає, що з'єднання між двома вузлами мережі не є постійним і існує лише тоді, коли трафік проходить через мережу.

3.2.2 Функції та компоненти VPN

Безпечний віртуальний VPN - це поєднання локальних мереж та персональних комп'ютерів через відкрите зовнішнє середовище для передачі інформації в єдиній віртуальній корпоративній мережі, що гарантує безпеку даних, які перебувають в обігу.

Під час підключення корпоративної локальної мережі до відкритої мережі існують два основні типи загроз безпеці:

- несанкціонований доступ до даних компанії, що передаються через відкриту мережу;
- несанкціонований доступ до внутрішніх ресурсів локальної мережі, отриманий зловмисником після несанкціонованого доступу до цієї мережі.

Захист інформації під час передачі по відкритим каналам зв'язку ґрунтується на таких основних функціях:

- автентифікація взаємодіючих сторін;
- криптографічне закриття (шифрування) даних, що передаються;
- перевірка достовірності та цілісності переданої інформації.

Ці функції характеризуються взаємозв'язком один з одним. Їх реалізація заснована на використанні методів захисту криптографічної інформації.

Для захисту локальних мереж та персональних комп’ютерів від несанкціонованих дій із зовнішнього середовища зазвичай використовуються

брандмауери для підтримки безпеки інформаційної взаємодії шляхом фільтрації двостороннього потоку повідомлень, а також виконуючи функції посередництва в обміні інформацією. Брандмауер розташований на інтерфейсі між локальною та відкритою мережами. Для захисту окремого віддаленого комп'ютера, підключеного до відкритої мережі, на цьому ж комп’ютері встановлюється програмне забезпечення брандмауера, і цей брандмауер називають персональним.[4]

3.2.3 Типи тунелів VPN

Захист інформації в процесі її передачі по відкритих каналах базується на побудові захищених віртуальних каналів зв'язку, так званих крипто захищених тунелів. Кожен з цих тунелів - це з'єднання, встановлене через відкриту мережу, через яку передаються пакети захищених криптографічних повідомлень.

1) PPTP VPN

Це протокол тунелювання базується на принципі з точки в точку - він створює тунель, захоплюючи дані. Це найпоширеніший тип технології, який дозволяє підключитися до мережі VPN через існуючі підключення до Інтернету. Цей варіант стане ідеальним рішенням для домашнього та професійного використання. Для нього не потрібно встановлювати додаткове обладнання, при цьому його можна використовувати в недорогих і простих програмах. Технологія PPTP VPN прекрасно сумісна з усіма операційними системами.

Незважаючи на велику кількість переваг, технології з протоколом PPP не можуть гарантувати користувачеві високий рівень безпеки, тому цей варіант не підходить для серйозних цілей та для впровадження в організаціях.

2) Site-to-Site VPN

Це найпоширеніший тип VPN в бізнесі, що працює за принципом маршрутизатор-маршрутизатор або хост-хост. Зокрема, цей варіант стає актуальним для компаній, що мають офіси в різних регіонах країни або в декількох країнах, що дозволяє зв’язати всі комп'ютери в одному ланцюзі. Під час використання VPN хост-хост компанія підключається до сервера іншої компанії

так само, як екстранет (VPN в одній мережі). Простіше кажучи, Site-to-Site VPN - це своєрідний міст, який з'єднує мережі в різних місцях, забезпечуючи безпечне з'єднання та Інтернет.

Ця система, як і PPTP, створює захищену мережу. Але на відміну від PPTP, шифрування здійснюється за допомогою спеціально розроблених пристроїв або за допомогою програм на обох кінцях мережі.

3) L2TP VPN

Це протокол тунелювання другого рівня, розроблений Cisco та Microsoft. Віртуальна приватна мережа, заснована на протоколі L2TP, поєднується з іншими протоколами, що гарантуватиме максимальну безпеку з'єднання. При використанні протоколу L2TP між двома точками з'єднання формується тунель, а також за допомогою використання іншого протоколу, наприклад IPsec, після чого інформація шифрується.

Діє L2TP як і PPTP. Ключова схожість - відсутність шифрування та основи на протоколі PPP. Єдина відмінність криється в захисті та безпеці даних - ця опція може гарантувати найбільш надійне та безпечне з'єднання.

4) IPsec

IPsec - це протокол VPN, який використовується для забезпечення максимальної безпеки мережі. Протокол встановлює своєрідний тунель до віддаленого хоста. Кожен сеанс тестується, пакети даних шифруються, так що протокол може гарантувати високий рівень безпеки з'єднання. Існує два режими роботи протоколу - тунельний і транспортний, які призначені для захисту даних між різними мережами. У транспортному режимі повідомлення всередині пакету даних шифруються, а в тунельному режимі весь інформаційний пакет зашифрований. Перевага використання IPsec полягає в тому, що він може бути використаний на додаток до інших протоколів, що значно покращує безпеку мережі.

Хоча IPsec є практичним і корисним протоколом, він має головний недолік - тривалий час установки клієнтської програми.

5) SSL та TLS

SSL і TLS - це два протоколи, які працюють в єдиній системі. SSL призначений для захисту пакетів даних, а TLS - безпеки на транспортному рівні. При використанні VPN з цими технологіями браузер працює як клієнт, користувач має доступ до спеціальних додатків по всій мережі. Активно використовується в онлайн-продажах, пропонуючи безпечний сеанс браузера на сервері за допомогою програми. Браузер підключається до SSL без проблем і додаткових дій з боку користувача.

6) MPLS VPN

MPLS - це мультипротокольна технологія комутації міток, яка широко використовується у службах VPN. Ідеальне рішення для підключення веб-сайту. Все це тому, що ця технологія є найбільш гнучкою з максимальними можливостями з точки зору адаптації. Він заснований на певних стандартах, що застосовуються для прискорення розподілу мережевих пакетів за кількома протоколами. Послуги з технологією MPLS налаштовані на роботу з провайдером, коли поєднується ряд сайтів і створюється VPN.

Недоліком цієї технології є те, що мережу налаштовувати набагато складніше, ніж при використанні інших протоколів. Складніше вносити зміни в додаток. В результаті послуги VPN, які підтримують протоколи MPLS, коштують користувача набагато дорожче, ніж інші протоколи.

7) Гібридна VPN

Як випливає з назви, ми говоримо про гібридний VPN, який поєднує IPSec і MPLS. Кожен із варіантів застосовується окремо на різних вузлах. У цей момент вузол дозволяє одночасно з'єднати два типи протоколів. Це робиться для того, щоб підвищити надійність MPLS за допомогою IPSec. Але для цієї мережі потрібно певне обладнання - роутер або захисний пристрій. З його допомогою дані створюють шифрування та тунель VPN.

Гібридні VPN ідеально підходять для великих організацій. Але всі ці функції сприяють тому, що вартість з'єднання вище. Використовуючи гібридну мережу, ви можете підключитися до центрального сайту через віддалений сайт. Хоча вони і дорогі, але вони найбільш гнучкі в плані налаштування.

8) Брандмауери на основі VPN

Брандмауери більшості виробників включають тунелювання та шифрування даних. Модуль шифрування додається до фактичного програмного забезпечення брандмауера.

До недоліків цього методу можна віднести високу вартість рішення з точки зору робочої станції та залежність від продуктивності обладнання, на якому працює брандмауер. На рисунку 3.2 показаний приклад поєднання брандмауера та VPN.[7]

Під час використання брандмауерів на основі ПК пам’ятайте, що ця опція підходить лише для невеликих мереж з обмеженою кількістю переданої інформації.

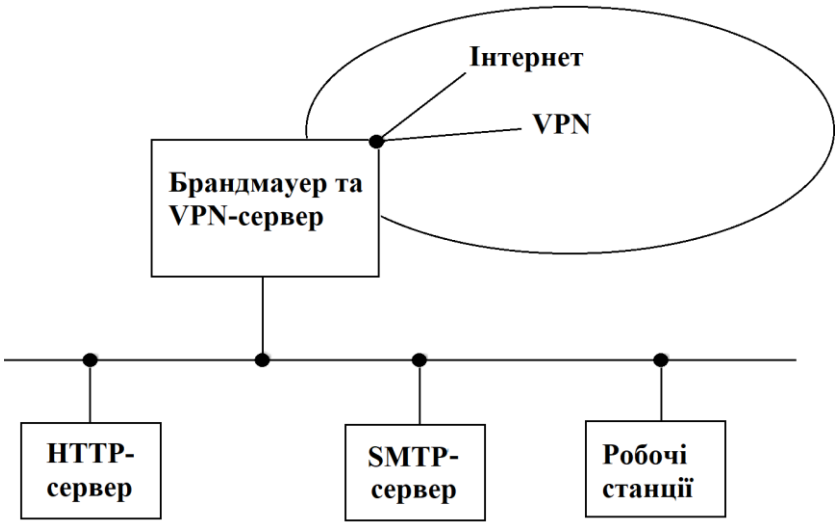

Рисунок 3.2 - Приклад поєднання брандмауера та VPN

Підводячи підсумок, можно сказати, щовибір найкращого варіанту тунелю VPN є кропітким завданням. Для того щоб зрозуміти тип VPN, який вам потрібен, вам потрібно визначити тип безпеки, який вам потрібен. Це вже залежить від того, хто ви: студент, власник малого чи великого бізнесу. Важливо визначити, чи достатньо простої системи безпеки для серфінгу в Інтернеті чи потрібна більш складна система, наприклад, гібридна. Важливим фактором є також вартість - скільки грошей ви готові виділити, щоб забезпечити безпечне підключення до Інтернету або до віддаленого серверу. Виходячи з усього цього, ви можно зробити правильний вибір.[5]

4 ПОБУДОВА ЛОКАЛЬНИХ МЕРЕЖ НА БАЗІ ОБЛАДНАННЯ MIKROTIK

4.1 Загальні відомості про MikroTik

MikroTik - це латвійський виробник мережевого устаткування. Компанія займається розробкою і продажем провідних і безпровідних мережевих маршрутизаторів, мережевих комутаторів, точок доступу, що називають RouterBOARD, а також операційних систем (RouterOS) і допоміжного програмного забезпечення.

Ці продукти відносяться до напівпрофесійного сегменту, який займає нішу між домашніми маршрутизаторами типу D-Link, TP-Link, Asus і професійним обладнанням типу Cisco і Juniper. У порівнянні з домашніми роутерами продукти MikroTik відрізняються значно більшою кількістю можливостей.

З професійним же обладнанням їх порівняти непросто, але низькі ціни роблять роутери MikroTik привабливими для малого і середнього бізнесу і навіть для деяких великих мережевих провайдерів.

При виборі маршрутизаторів, комутаторів або точок доступу складно порівнювати MikroTik з роутерами типу D-Link, TP-Link, бо безпека і надійність їх програмного забезпечення та потужність апаратної частини явно недостатні для організації безпечної комп'ютерної мережі, навіть на рівні малого чи середнього бізнесу.

З обладнанням Cisco, порівнювати теж досить складно, тому що в першу чергу це обладнання абсолютно іншого класу. По функціональності обладнання MikroTik можна порівнювати з обладнанням Cisco, адже обидва виробники закладають у своє обладнання масу можливостей, зокрема, реалізацію обладнанням різних мережевих завдань, наприклад, з'єднань VPN різного типу, налаштування міжмережевих екранів, реалізацію безшовного роумінгу, гнучкість налаштувань, тощо. Складно посперечатися з високою надійністю систем Cisco і його висококласною цілодобовою підтримкою, чого явно немає в MikroTik, є ще маса переваг Cisco, але як показує практика, якщо споживачем є не величезна

корпорація, а малий і середній бізнес, то ключовим питанням стане ціна, а цей пункт кардинально відрізняє ці дві компанії. Для порівняння, аналог обладнання MikroTik від Cisco буде за ціною вище в 5-10 разів, наприклад, порівняємо два приблизно аналогічних по можливості бюджетних маршрутизатора від цих двох фірм, при цьому MikroTik RB2011UiAS-IN обійдеться в 2500 грн, а аналогічне обладнання Cisco Catalyst 2960C вийде в ціну 11000 грн, тобто ціна різниться в 4,5 рази, при дуже схожих характеристиках. Звідси можна зробити висновок, що малі та середні компанії віддадуть перевагу більш дешевому обладнанню, тим більше, що необхідно закупити далеко не один елемент комп'ютерної системи, що дозволить заощадити не одну тисячу доларів.

На своєму рівні головним конкурентом MikroTik є виробник Ubiquiti. Якщо необхідно забезпечити якісне покриття Wi-Fi з більш стабільно працюючим безшовним роумінгом, то необхідно використовувати точки доступу Ubiquiti, бо радіомодулі Ubiquiti, як правило, більш потужні, а реалізована технологія MIMO і безшовний роумінг, більш якісно працюють по відношенню до конкурента. Якщо ж основним завданням є побудова безпечної та відмовостійкої мережі, то переваги мають рішення компанії MikroTik, адже воно має більш гнучке налаштування обладнанням з великими можливостями і при правильному налаштуванні, як показує практика, більш стабільним і таким, що забезпечує захист від атак. [10]

4.2 Mikrotik RouterOS - опис і можливості

Mikrotik RouterOS - це спеціалізована операційна система, призначена виключно для побудови багатофункціональних маршрутизаторів, фаєрволів, бриджів, базових станцій, vpn-серверів, web-серверів та інших пристроїв управління мережами. При цьому працювати операційна система може як на апаратних платформах Mikrotik RouterBoard, побудованої як правило на процесорах PowerPC і Atheros, так і на обладнанні побудованому на базі x86 архітектури, простіше кажучи - звичайні персональні комп'ютери.

Устаткування підтримуване Mikrotik Router OS:

- архітектура i386;
- SMP - підтримка декількох ядер і декількох процесорів;
- мінімальна кількість оперативної пам'яті 32 Мб (максимальне 2 Гб);
- підтримка IDE, SATA, USB накопичувачів з об'ємом від 64Мб;
- мережеві карти підтримувані ядром linux v2.6 kernel (PCI, PCI-X).

Не дивлячись на те, що сама операційна система побудована на ядрі linux, вона не є OpenSource проектом. Код Mikrotik Router OS не доступний громадськості і отримати доступ до командного рядка linux, не представляється можливим. Встановити RouterOS можна кількома способами, так на персональний комп'ютер, вона може бути встановлена за допомогою установочного CD диска, iso файлу, який можна знайти на сайті компанії Mikrotik або через мережу, за допомогою утиліти Netinstall, яку так само можна знайти на сайті розробника. Установка на спеціалізоване обладнання RouterBoard.

Після установки, є багато варіантів подальшої конфігурації і подальшого управління Mikrotik Router OS і всіма функціями:

- MAC based - доступ до пристрою на рівні MAC адреси;
- WinBox - утиліта для Windows OS;
- WebBox - вебінтерфейс;
- Webfig - розширений конфігураційний веб-інтерфейс;
- Командний рядок (консоль) з вбудованою підтримкою скриптів і працюй по telnet і ssh протоколам;
- API - можливість створення власних додатків для налаштування або моніторингу мережі.

Підтримується збереження / відновлення і імпорт всіх налаштувань конфігурації, як в бінарний файл, так і в зрозумілий людині текстовий формат.

І як вже говорилося вище, Mikrotik RouterOS це досить потужний інструмент для створення мереж і їх управлінням, що включає в свій арсенал величезна кількість функцій для роботи практично з усіма можливими мережевими протоколами. Підтримуються такі функції для роботи з протоколом TCP / IP як:

1) Firewall:
   - NAT (Network Address Translation) - механізм розподіл пакетів з реалізацією функцій SNAT і DNAT;
   - внутрішній розподіл і маршрутизація пакетів;
   - фільтрація по IP адресами, діапазонами адрес, портів і їх діапазонами, протоколам, інтерфейсів, маркування пакетів і багато іншого;
   - списки адрес;
   - повна підтримка IPv4 і IPv6;
   - PCC (Per Connection Classifier) - механізм розподілу навантаження.
2) Routing:
   - статична маршрутизація;
   - віртуальна маршрутизація (VRF);
   - маршрутизація на базі політик;
   - маршрутизація на базі інтерфейсів;
   - динамічні протоколи маршрутизації RIP v1 / v2, OSPFv2, BGP v4 і RIPng, OSPFv3, BGP для IPv6 протоколу.
3) VPN і тунелі:
   - IPsec - IP security AH і ESP протоколи, з підтримка апаратного шифрування на деяких моделях обладнання RouterBoard;
   - PTP (Point to Point) протоколи, включаючи OpenVPN, PPTP, PPPoE, L2TP, SSTP з підтримкою PAP, CHAP, MSCHAPv1 і MSCHAPv2 авторизації;
   - підтримка простих тунелів по протоколам IP2IP і EoIP в мережах IPv4 і IPv6;
   - підтримка віртуальних мереж VLAN;
   - тунелі на базі MPLS.
4) DHCP:
   - базовий DHCP сервер з підтримкою IPv6 (DHCPv6-PD);
   - DHCP клієнт з підтримкою IPv6 (DHCPv6);
   - статичний і динамічний DHCP;

- персональні DHCP настройки.

5) QoS:
   - можливість динамічного керування смугою пропускання для IP, протоколу, підмережі, порту і ланцюжки за допомогою протоколу HTB (Hierarchical Token Bucket);
   - Simple queues (прості черзі) для швидкої реалізації функції QoS;
   - динамічне вирівнювання швидкості клієнта (PCQ).
6) Proxy:
   - вбудований FTP і HTTP / HTTPS проксі-сервер з можливістю кешування;
   - прозорий DNS і HTTP проксі-сервер;
   - підтримка SOCKS протоколу;
   - DNS static записи;
   - підтримка Parent proxy;
   - список доступу Access control list.
7) ISDN:
   - ISDN dial-in / dial-out;
   - підтримка протоколів авторизації PAP, CHAP, MSCHAPv1 і MSCHAPv2;
   - підтримка протоколів Cisco HDLC, x75i, x75ui, x75bui;
   - дозвон на вимогу.

Реалізована в Router OS і повна підтримка роботи з бездротовими протоколами:

1) Wireless:
   - бездротової клієнт або точка доступу за протоколами IEEE802.11a/b/g/n;
   - повна підтримка протоколу IEEE802.11n;
   - розроблені компанією протоколи Nstreme і Nstreme2;
   - NV2 протокол;
   - повна підтримка функцій протоколу бездротового розподілу WDS;

- створення віртуальних точок доступу Virtual AP;
- Wireless client roaming;
- підтримка протоколів HWMP + Wireless MESH і MME wireless routing.

2) Безпека безпровідних мереж:
   - протоколи захищеного бездротового доступу WEP, WPA, WPA2;
   - підтримка AES і TKIP;
   - списки доступу Access control list.
3) Hotspot
   - можливість побудови Plug-n-Play точок колективного користування Internet;
   - авторизація користувачів локальної мережі;
   - облік користувачів;
   - можливість створення зон;
   - можливість завдання швидкості, часу роботи клієнта та ін.

Серед інших функцій управління мережевим оточенням доступних в цій операційній системі:

- Bridge - можливість створення мостів між інтерфейсами з фільтрацією трафіку, що проходить;
- Dynamic DNS - можливість роботи з сервісами динамічних DNS серверів, таких як NO-IP або DynDNS;
- VLAN - підтримка IEEE802.1q Virtual LAN через Ethernet і через бездротові інтерфейси, з можливістю побудови множинних VLAN-ів і побудова VLAN-мостів;
- RADIUS (Remote Authentication Dial In User Service) - мережевий протокол, що забезпечує централізовану аутентифікацію користувачів;
- MPLS - механізм в високопродуктивної мережі здійснює передачу даних за допомогою міток;
- NTP (Network Time Protocol) - сервер і клієнт синхронізації часу. Можливості синхронізації з GPS системою;
- VRRP - підтримка протоколу VRRP v2 і v3;

- UPnP - повна підтримка протоколу Universal Plug-and-Play;
- SDSL - підтримка Single-line DSL.

І це далеко не повний список можливостей Mikrotik Router OS, крім того, він постійно поповнюється з виходами свіжих версій операційної системи.

Не можна не відзначити кілька ексклюзивних протоколів використовуваних тільки на обладнанні Mikrotik і підтримувані програмним забезпеченням цієї фірми.

MNDP (The MikroTik Neighbor Discovery Protocol) - дозволяє максимально спростити настройку мережі та її управління, даючи можливість кожному маршрутизатора MikroTik, автоматично отримувати інформацію про мережі і деякі настройки від інших пов'язаних в одну мережу пристроїв MikroTik.

Основні особливості MNDP:

- працює на рівні IP з'єднання;
- працює на всіх не динамічних інтерфейсів;
- розподіляє основну інформацію про версії програмного забезпечення;
- поширення інформації про особливості настройки, які можуть бути прийняті іншими маршрутизаторами MikroTik або під управлінням Mikrotik Router OS.

M3P (MikroTik Packet Packer Protocol) - протокол оптимізації швидкості передачі даних, застосовуваний в бездротових мережах для передачі наприклад, VoIP трафіку, який використовує малі розміри пакету, близько 100 байт.

Основні особливості M3P:

- включення з інтерфейсу налаштувань;
- інші маршрутизатори, котрі підтримують MikroTik Neighbor Discovery Protocol транслюватимуть M3P настройки;
- значно збільшує доступність смуги пропускання по протоколам бездротового зв'язку.

Так само серед іншого, в Router OS є багато корисних інструментів, набір яких включає в себе всілякі вбудовані мережеві утиліти для моніторингу стану мережі.

В Mikrotik Router OS також є вбудовані утиліти:

- ping, traceroute;
- bandwidth test, ping flood;
- packet sniffer, torch;
- telnet, ssh;
- відправка E-mail і SMS про стан мережі;
- автоматичне виконання скриптів;
- file Fetch tool;
- advanced traffic generator.

Mikrotik Router OS, не є OpenSource проектом і поширюється виключно на комерційній основі. Устаткування компанії, побудоване на платформах Mikrotik RouterBoard, як правило поставляється з уже встановленою Router OS з ліцензією одного з чотирьох рівнів (Level 3, 4, 5 або 6) і не вимагають придбання ключа. При цьому, в разі необхідності є можливість підвищення рівня ліцензії за додаткову плату. Порівняльну таблицю рівнів ліцензії Mikrotik Router OS наведено в таблиці 4.1.

Підводячи підсумок всього вищесказаного, можна резюмувати, що MikroTik RouterOS - це автономна і самодостатня мережева операційна система досить високого рівня, здатна вирішувати величезну кількість задач пов'язаних з мережевими рішеннями. [11]

Таблиця 4.1 — Порівняльна таблиця рівнів ліцензії Mikrotik Router OS

Рівень ліцензії	0 (демо)	1 (безко-штовно)	3 (WISP CPE)	4 (WISP)	5 (WISP)	6 (Controller)
Ціна	без ключа	Потрібна реєстрація		$45	$95	$250
Оновлення до	-	-	ROS v6.x	ROS v6.x	ROS v7.x	ROS v7.x
Тих. підтримка в налаштуванні	-	-	-	15 днів	30 днів	30 днів
Бездротова точка доступу	24 год. trial	-	-	так	так	так
Бездротовий клієнт і міст	25 год. trial	-	так	так	так	так
Протоколи маршрутизації RIP, OSPF, BGP	26 год. trial	-	так	так	так	так
EolP тунелі	27 год. trial	1	не обмежено	не обмежено	не обмежено	не обмежено
PPPoE тунелі	28 год. trial	1	200	200	500	не обмежено
PPTP тунелі	29 год. trial	1	200	200	500	не обмежено
L2TP туннелі	30 год. trial	1	200	200	500	не обмежено
OVPN тунелі	31 год. trial	1	200	200	не обмежено	не обмежено
VLAN інтерфейси	32 год. trial	1	не обмежено	не обмежено	не обмежено	не обмежено
Користувачів HotSpot	33 год. trial	1	1	200	500	не обмежено
RADIUS клієнти	34 год. trial	-	так	так	так	так
Черги	35 год. trial	1	не обмежено	не обмежено	не обмежено	не обмежено
Web-proxy	36 год. trial	-	так	так	так	так
Активних сесій Usermanager	37 год. trial	1	10	20	50	не обмежено
Кількість KVM підключень	ні	1	не обмежено	не обмежено	не обмежено	не обмежено

Переваги мережевого обладнання MikroTik:

- Співвідношення ціна-якість-функціональність. Вирішує більшість мережевих завдань: Маршрутизація, комутація, Wi-Fi, безшовна мережа, RADIUS, VPN, LTE та ін. При цьому аналогічні рішення від конкурентів коштують в рази дорожче, наприклад, відносно Cisco, аналог буде коштувати мінімум в 10 разів дорожче.
- Дистрибутив об'ємом 15 Мб.
- Зручність і простота сприйняття інтерфейсу.
- Швидкість і зручність настройки.
- Постійні оновлення (17 оновлень за 2019 рік).
- Швидкість виправлення помилок. Наприклад, після виявленої вразливості в протоколі TLS, експлуатуючи яку зловмисники могли обійти систему аутентифікації і отримати віддалений доступ до пристрою, розробникам знадобилося менше ніж за 24 годин з моменту виявлення вразливості, щоб усунути пролом в ОС, протестувати і випустити оновлення, яке б закривало цю уразливість.
- Широкий температурний режим (40 .. + 70). При тому що у конкурентів показники зазвичай на рівні 0 ... +40.
- Хороший функціонал в промислових рішеннях: LTE, GPS, LORA, 60G; при цьому конкуренти Sierra Wireless, Teltonika і ін. в рази дорожче і менш гнучкі в функціоналі.
- Дуже функціональний і гнучкий firewall, зручний інтерфейс iptables.
- Гарна стійкість до атак типу DoS.

Основні недоліки:

- Оновлення, з новими оновленнями іноді з'являються і інші помилки, які все ж надалі усуваються, але вони є.
- Не реалізовані технології: MU-MIMO, Beamforming, High Density WiFi, 5GHz offloading, Deep analytics

- Технологія 802.11ac wave 2 - не дає належного результату пропускаемости каналу в 2,34 Гбіт / с.
- Використання зовнішніх блоків живлення в rack-mount версіях.
- Бракує опцій безпеки: URL-фільтрація, Antivirus/antimalware, IDS/IPS.[12]

4.3 Порівняння аналогів маршрутизаторів MikroTik та Ubiquiti

Порівняння маршрутизаторів середнього класу Mikrotik RB4011iGS + RM та Ubiquiti EdgeRouter 12. У цьому розділі ми спробуємо розібратися, чи є різниця між ними та саме в чому різниця.

MikroTik RB4011iGS + RM - потужний гігабітний маршрутизатор для малого та середнього бізнесу. Оснащений послідовним портом RJ45, 10 гігабітними портами Ethernet, слотом SFP+ та 12 світлодіодами (відображається робота кожного порту та потужність) для полегшення усунення несправностей. Оптичний порт використовується для створення мережевого каналу зв'язку на великі відстані, зокрема для підключення оптичних SFP + модулів зі швидкістю 10G.

Він працює під управлінням чотирьохядерного процесора AL21400 (32-бітна архітектура ARM) з тактовою частотою 1,4 ГГц. Має великий об'єм оперативної пам’яті (1 Гб) і пам'ять для зберігання параметрів і даних (512 МБ NAND). За порти комутації мікросхем RTL8367S відповідальний.

RB4011iGS + RM підтримує такі функції маршрутизації під управлінням попередньо встановленої операційної системи RouterOS 5:

- Двостороннє виявлення переадресації (BFD);
- Протокол прикордонного шлюзу (BGP);
- Протокол управління Інтернет-групами (IGMP);
- Власний протокол MME (Mesh Made Easy);
- Незалежна від протоколу багатоадресна передача (Multicast);
- Динамічний протокол маршрутизації OSPF версії 2 (RFC 2328);

- Мережевий протокол RIP версії 1 (RFC 1058) або версії 2 (RFC 2453).

У своїй роботі пристрій використовує протоколи IPsec для захисту даних, що передаються і з високим рівнем продуктивності, підтримує апаратне шифрування AES.

Нижче, в таблиці 4.2, приведені результати тесту продуктивності апаратного шифрування при використанні технології IPSec з різними алгоритмами і типами шифрування (AES-128, AES-256, SHA1, SHA256). [13]

Таблиця 4.2 – Результат тестування IPsec на Mikrotik RB4011iGS+RM

RB4011iGS+RM		AL21400 IPsec throughput					
Mode	Configuration	1400 byte		512 byte		64 byte	
		kpps	Mbps	kpps	Mbps	kpps	Mbps
Single tunnel	AES-128-CBC + SHA1	140.8	1577.0	141.2	578.4	139.9	71.6
256 tunnels	AES-128-CBC + SHA1	192.7	2158.2	200.5	821.2	203.4	104.1
256 tunnels	AES-128-CBC + SHA256	192.4	2154.9	200.5	821.2	203.4	104.1
256 tunnels	AES-256-CBC + SHA1	180.0	2016.0	188.2	770.9	190.3	97.4
256 tunnels	AES-256-CBC + SHA256	180.0	2016.0	188.2	770.9	190.3	97.4
256 tunnels	AES-128-GCM	192.7	2158.2	202.2	828.2	203.4	104.1

Ubiquiti EdgeRouter 12 - потужний гігабітний маршрутизатор для малого та середнього бізнесу. Оснащений десятьма керованими портами RJ45 Gigabit Ethernet, які забезпечують з'єднання з входом 24 В PoE на порт 0 і виходом з контуру 24 В PoE на порт 9. А також 2 гігабітні SFP-порти для оптичних підключень. Передбачений послідовний порт для управління пристроєм через інтерфейс командного рядка (CLI).

PoE порти:

- PoE In (1) 24V Passive PoE Port, 2-pair (4, 5+; 7, 8-);
- PoE Out (1) 24V Passive PoE Port, 2-pair (4, 5+; 7, 8-).

Маршрутизатор оснащений чотири ядерним процесором MIPS64 з тактовою частотою 1 ГГц. Користувач має 1 ГБ оперативної пам’яті DDR3, 4 Гб eMMK та 8 МБ пам'яті SPI NOR для зберігання даних та параметрів.

EdgeRouter 12 підтримує комутацію рівня 2 з двома внутрішніми свічами. Пропускна здатність досягає 3 400 000 пакетів в секунду, розмір пакета - 64 байт і 6,8 Gbps для пакетів 1518 байт і більше.

Для масштабованої конфігурації використовується операційна система Ubiquiti EdgeOS або система управління мережею Ubiquiti UNMS.

Операційна система EdgeOS має такі функції:

- підтримка статичних маршрутів та протоколів маршрутизації OSPF, RIP та BGP;
- політики брандмауера та правила NAT;
- DHCP;
- Quality of Service (QoS);
- інструменти управління мережею та моніторинг; повна підтримка IPv6;
- конфігурація різними способами: графічним інтерфейсом або командним рядком.

На жаль, виробник не надає результатів тестувань IPSec, тож порівняти швидкість роботи з MikroTik немає змоги. [14]

Отже, як ми бачимо в таблиці 4.3, моделі мають однакову кількість портів, Ethernet - 10 x GigabitEthernet. Об'єм оперативної пам’яті становить 1 ГБ, на цьому схожість закінчується.

Ми можемо бачити, що потужність процесора різна, Mikrotik в цьому випадку з 1,4 ГГц здається привабливішим, ніж Ubiquiti 1 ГГц. ER-12 має 4 Гб ПЗУ, на відміну від 512 Мб RB4011iGS. Щодо пакетної продуктивності IPSec для різних розмірів пакету та умов обробки, ми не можемо зробити висновок, враховуючи відсутність інформації від Ubiquiti. Можливо, в майбутньому виробник або тестові лабораторії нададуть цю інформацію. Але однозначно можна сказати, що апаратне шифрування Mikrotik, користується перевагою при організації захищених каналів даних, IPSec, організації VPN-мереж з

технологіями OVPN, SSTP та іншими тунельними протоколами, а також він більш стабільно реагує на різні атаки спрямовані на «відмова в обслуговуванні».

Що стосується цінової політики, то варто відзначити більш низьку ціну MikroTik - 180$, порівняно з ціною Ubiquiti – 250$, незважаючи на те, що продуктивність MikroTik в рази вища.

Таблиця 4.3 – Порівняння маршрутизаторів MikroTik RB4011iGS+RM та Ubiquiti EdgeRouter 12

Характеристики	Пристрої	
Виробник	MikroTik	Ubiquiti
Модель	RB4011iGS+RM	EdgeRouter 12 (ER-12)
Ціна	182,70 $	257,92 $
Процесор	AL21400	MIPS64
Номінальна частота процесора	1.4 GHz	1 GHz
Кількість ядер процесора	4	4
Об'єм оперативної пам'яті	1 GB DDR3 RAM	1 GB DDR3 RAM
Розмір сховища даних	512 MB	4 GB eMMC, 8 MB SPI NOR
Тип сховища даних	NAND	FLASH
Інтерфейси	10 x Gigabit Ethernet портов, 1 x 10 Gbps SFP+, 1 x RJ45 серийный порт	10 x Gigabit Ethernet портов, 2 x 1 Gbps SFP, 1 x RJ45 серийный порт, 1 x USB
Операційна система	RouterOS	EdgeOS
Рівень ліцензії	5	—
Максимальне енергоспоживання	18 W (без підключень), 33 W (max power)	20 W (без PoE Output)
Підтримка PoE	PoE in: Passive PoE; PoE out: Ether10, 802.3af/at	PoE In: Passive PoE, 2-pair (4, 5+; 7, 8-); PoE Out: Passive PoE Port, 2-pair (4, 5+; 7, 8-)
Діапазон температур	-40°C ... +70°C	-10...+50°C
Продуктивність	При розмірі пакета 64 байта - 5509 kpps; при розмірі пакета: 1518 байт і більше - 9.7 Gbps (швидкість лінії)	При розмірі пакета 64 байта - 3400 kpps; при розмірі пакета: 1518 байт і більше - 6.8 Gbps (швидкість лінії)

Яку модель вибрати, треба вирішити враховуючи бюджет, продуктивність та особливості, які можна знайти: у нашому прикладі RouterOS дозволяє якісно керувати трафіком та мати можливість гнучких, але більш складних налаштувань, або EdgeOS, з інтуїтивним веб-інтерфейсом та прекрасною графікою.

4.4 Вразливості Mikrotik Router OS

Останнім часом розробникам MikroTik довелося по-працювати, все через підвищеного до них інтересу з боку хакерів, які знайшли уразливості, що дозволяли на обладнанні Mikrotik реалізовувати видобуток криптовалют, робити їх частиною ботнетів, перехоплювати трафік і заражати собі подібних. Всьому виною - нові вразливості, знайдені в продукції MikroTik.

Звичайно, всі уразливості вже виправлені виробником, але поговорити про них варто. Бо більшість користувачів MikroTik не поспішають самостійно оновлювати прошивку, а як наслідок їх пристрої залишаються уразливими.

Вразливості, як і завжди, можна розділити на критичні і некритичні. Почнемо з найменш критичних. Такими вразливими можна вважати і такі, що були виявлені в серпні 2018 року команда Tenable Research CVE-2018-1157, CVE-2018-1159, CVE-2018-1158. Всі вони пов'язані з ушкодженнями пам'яті, але експлуатувати їх може тільки авторизований користувач.

CVE-2018-1156. Проблема пов'язана з механізмом оновлення RouterOS. При її експлуатації авторизований зловмисник може виконати шкідливий код.

CVE-2018-10070. Дозволяє не авторизованим зловмисникам вичерпати ресурси ЦП і ОЗУ, відправляючи запити на порт FTP. Результатом буде перезавантаження без належного процесу відключення.

CVE-2019-5599 (SACK Slowness) - дозволяє викликати фрагментацію карти відправлених пакетів при обробці спеціальної послідовності SACK в рамках одного TCP-з'єднання і викликати виконання ресурсномісткою операції перебору списку, що може, в свою чергу, викликати небажане перевантаження процессора, а як наслідок, збої в роботі.

Переходимо до найбільш небезпечних вразливостей.

CVE-2018-10066 дозволяє перехоплювати клієнтський трафік. Вразливість пов'язана з відсутністю перевірки сертифіката OpenVPN.

CVE-2018-7445. Це вразливість, яка дозволяє зловмисникам отримати доступ до роутера і виконувати шкідливий код. Атака починається з відправлення запиту

на сесію NetBIOS. Функцію безпеки, яка не дозволяє виконувати код з області пам'яті, вдалося обійти методом зворотно-орієнтованого програмування (ROP). В результаті вдалося відзначити область пам'яті як придатну для запису і виконання.

CVE-2019-11477 (SACK Panic) - проблема проявляється в ядрах Linux починаючи з 2.6.29 і дозволяє викликати крах (panic) ядра через відправку серії SACK-пакетів через виникнення цілочисельного переповнення в обробнику.

Дві уразливості були виявлені і розкриті MikroTik 11 вересня 2019 роки (CVE-2019-3976 і CVE-2019-3977) і ще двоє 13 вересня 2019 роки (CVE-2019-3978 і CVE-2019-3979). Спільне використання цих вразливостей дозволило знизити версію RouterOS, чим створити прогалину в безпеці комп'ютерної мережі. [15]

Якщо за всі ці вразливості несе відповідальність виробник, то у розділі 4.5 ми розглянемо, як саме ми можемо вплинути на те, щоб спроби зловмисників проникнути через WAN-порт роутера у внутрішню мережу не увінчалися успіхом.

4.5 Рекомендації по налаштуванню центрального маршрутизатора MikroTik з урахуванням забезпечення безпеки корпоративної мережі

4.5.1 Модернізуємо стандартні налаштування Router OS

1) Налаштовуємо автоматичне закриття сесії. За замовчуванням тривалість сесії встановлено на рівні 24 години, але з'єднання не завжди коректно закриваються, а короткі сесії висять довго, займаючи цим оперативну пам'ять.

З цієї причини встановлюємо час життя сесії 1 годину, якщо після закінчення цього часу сесія буде активна, вона сама продовжується (Рис. 4.1). Як результат ми розвантажимо оперативну пам'ять маршрутизатора.

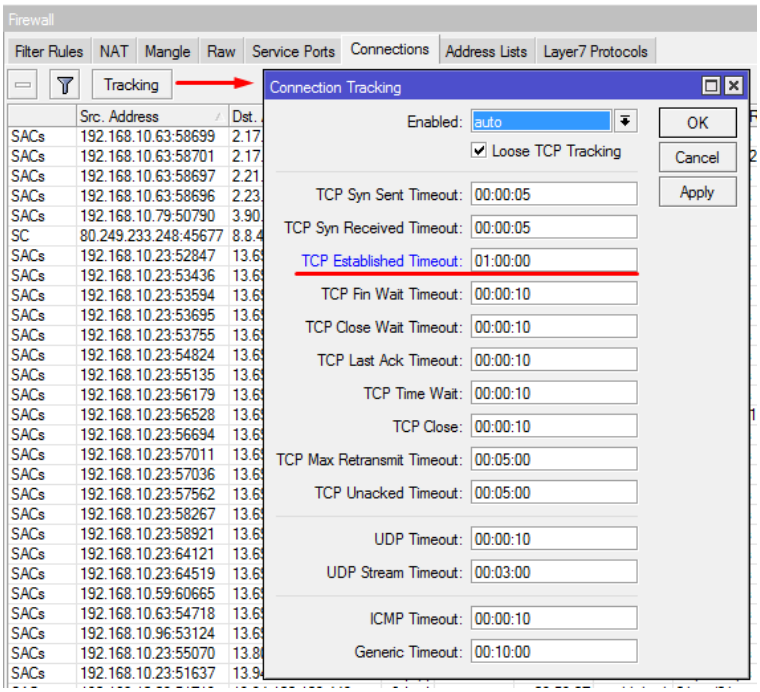

Рисунок 4.1 - Налаштування автоматичного закриття сесії

2) В окремих випадках зустрічаються проблеми оновлення орендованої ip-адреси у деяких специфічних пристроїв, наприклад, часто зустрічається у продукції Apple.

За стандартом встановлено час оренди 10 хв., Але в разі, якщо зустрічається дана проблема, або в ім'я уникнення таких проблем, необхідно встановити час життя орендованої ip-адреси, якщо це корпоративна мережа - на значення 3 дні, якщо гостьова - на значення 1 година (Рис. 4.2). Можна використовувати таку команду:

/ip dhcp-server set lease-time=1h

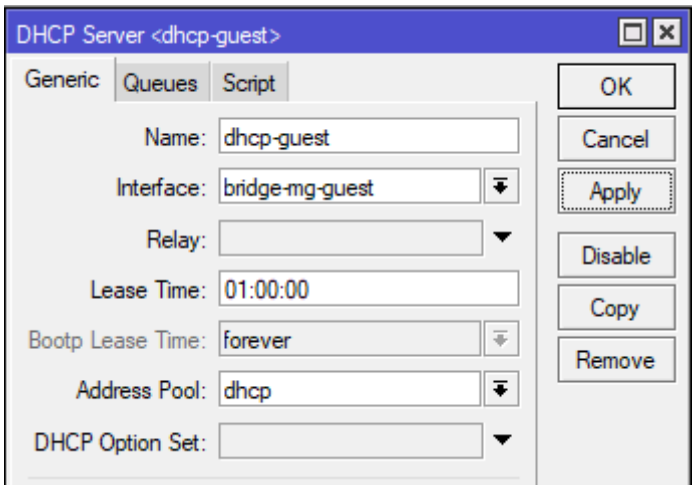

Рисунок 4.2 - Налаштування DHCP-сервера для гостьової мережі

3) Відключаємо служби які не збираємося використовувати.

Необхідно закрити всі невживані служби, особливо доступ до роутера через web-інтерфейс, telnet та ssh. Так само необхідно в обов'язковому порядку замінити стандартні порти служби winbox, ssh та інших, якщо їх використання необхідне, а також додати список ip-адрес з яких можливе підключення (Рис. 4.3).

```
/ip service {
set telnet disabled=yes
set ssh disabled=yes
set ftp disabled=yes
set www disabled=yes
set api disabled=yes
set api-ssl disabled=yes
}
```

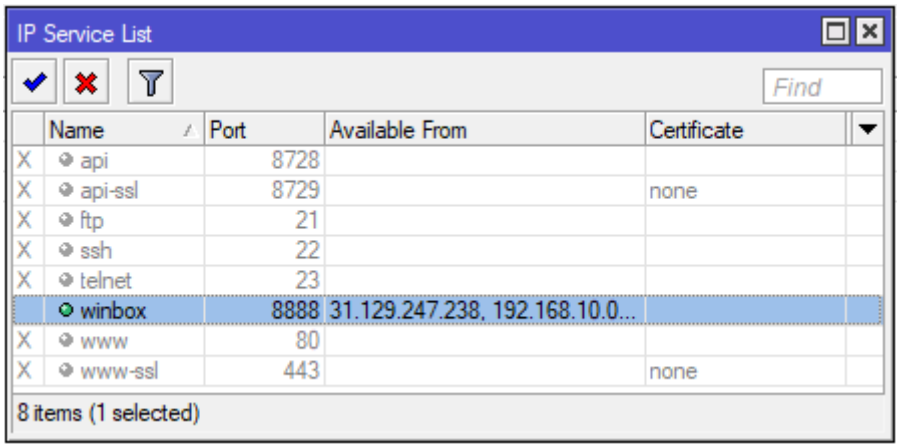

Рисунок 4.3 - Змінюємо стандартні порти та вимикаємо незастосовані

4) Вимкнути всі невикористовувані сервісні порти, щоб виключити можливе несанкціоноване проникнення (Рис. 4.4).

Зробити це можна в графічному інтерфейсі або командою:

```
/ip firewall service-port
set ftp disabled=yes
set tftp disabled=yes
set irc disabled=yes
set h323 disabled=yes
set sip disabled=yes
```

set pptp disabled=yes

set dccp disabled=yes

set sctp disabled=yes

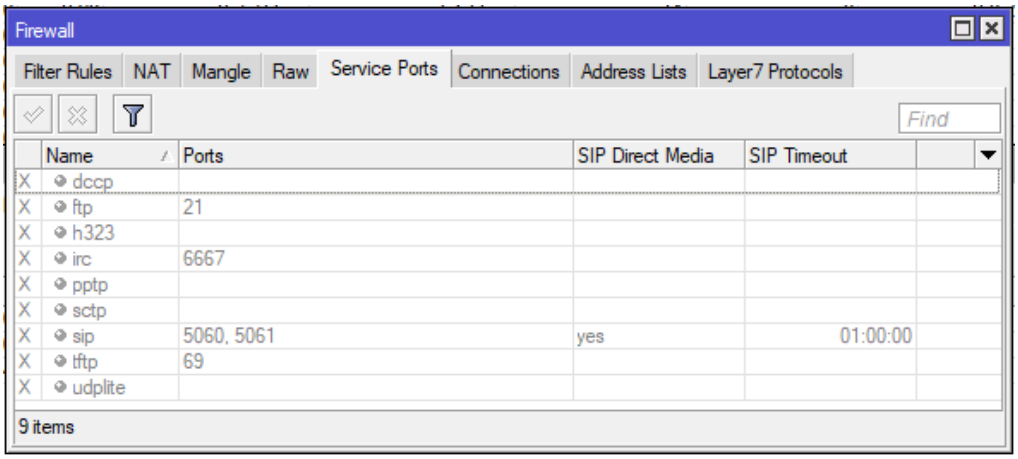

Рисунок 4.4 - Вимикаємо незастосовані сервісні порти

5) Змінюємо стандартного користувача admin і встановимо йому надійний пароль.

Стандартний користувач admin, полегшить життя тим, хто вирішить спробувати підібрати пароль до облікового запису адміністратора.

Додаємо нового користувача з правами адміністратора і видаляємо старий обліковий запис (Рис. 4.5).

/user add name=Gadmin password=Passw12 group=full

/user remove admin

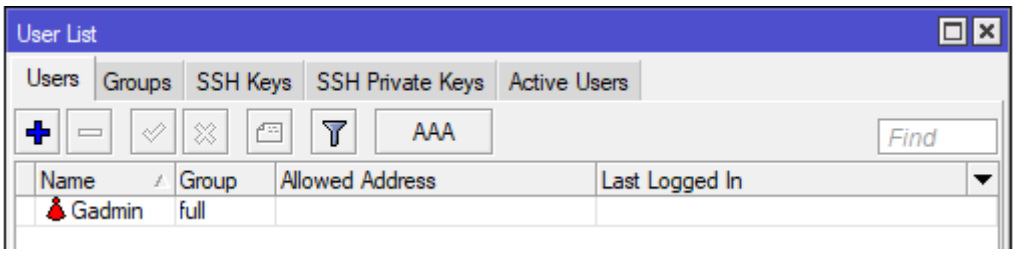

Рисунок 4.5 - Створення нового користувача

6) У стандартних налаштуваннях правила NAT працюють тільки під час взаємодії з глобальною мережею, але не функціонують з локальної мережі, з цієї причини додаємо глобальне правило:

/ip firewall nat add chain=srcnat action=masquerade out-interface-list=LAN srcaddress-list=local_net comment="NAT for LAN”

Після цього додаємо в Address List local_net використовувані локальні підмережі:

/ip firewall address-list add address=192.168.0.0/24 list=local_net

/ip firewall address-list add address=192.168.10.0/24 list=local_net

/ip firewall address-list add address=192.168.40.0/24 list=local_net

Додамо ще один Address List під ім'ям WAN _IP і додаємо туди нашу зовнішню IP-адресу:

/ip firewall address-list add address=x.x.x.x list=WAN _IP

Як результат, правило «проброса порту» буде виглядати так:

/add action=dst-nat chain=dstnat dst-address-list= WAN -IP dst-port=80

protocol=tcp to-addresses=192.168.0.10 comment="Port-forward"

За замовчуванням після запиту до центрального роутера, сервер відповідає напряму до хоста, що до неї звертався (Рис. 4.6).

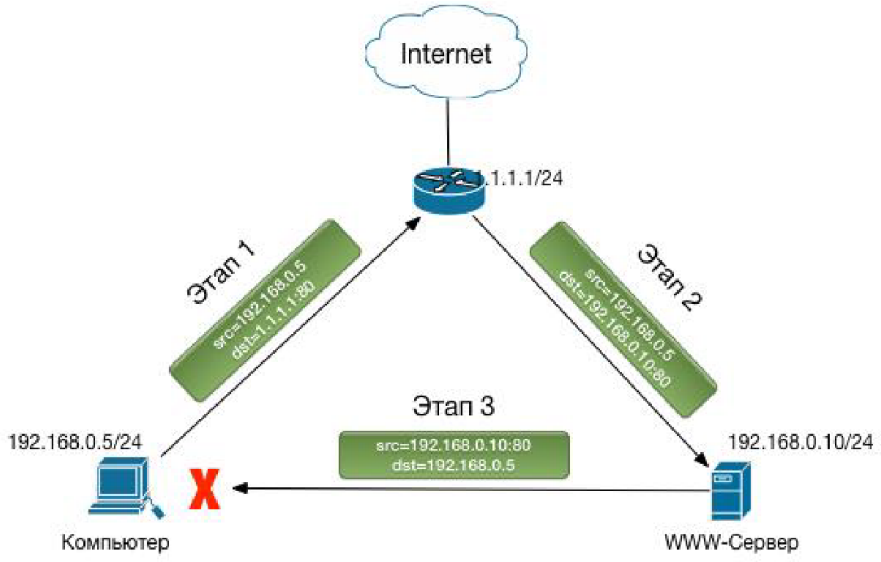

Рисунок 4.6 - Стандартний NAT в локальній мережі

Після встановлення правила в NAT, усі пакети, як вхідні, так і вихідні, будуть контролюватись центральним маршрутизатором (Рис. 4.7).

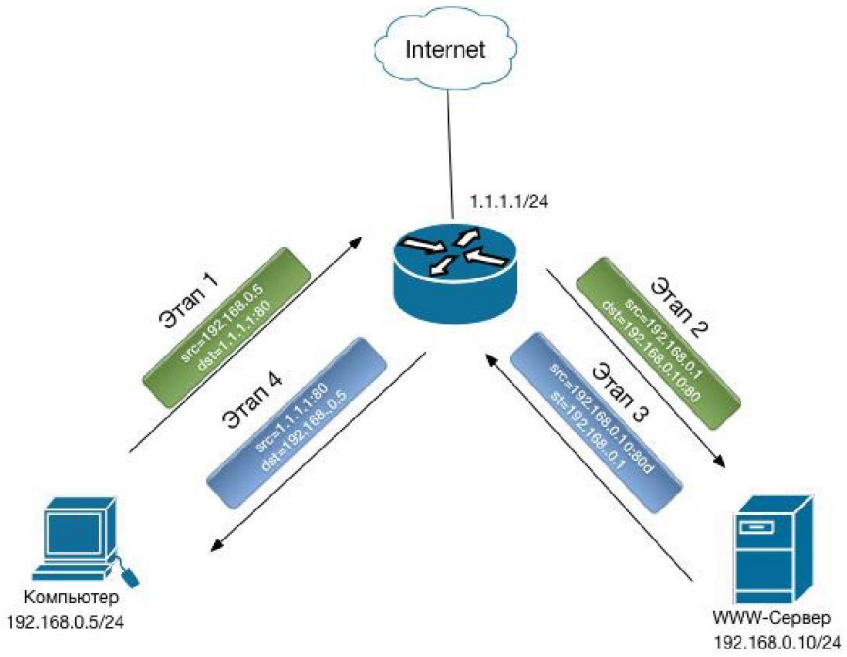

Рисунок 4.7 - Задіємо правила NAT в локальній мережі

7) NTP клієнт за замовчуванням перевіряє ліквідність ip-адреси доменних імен серверів NTP тільки один раз при ввімкненні обладнання. За для впевненості в точному відображенні журналу подій, встановимо автоматичне оновлення NTP-серверів кожні 12 годин.

Як рішення можна використовувати такий скрипт:

/system script add name= “Update NTP Server” policy=read,write,test source="

:local ntpcura [/system ntp client get primary-ntp];

:local ntpcurb [/system ntp client get secondary-ntp];

:local ntpipa [:resolve 0.ua.pool.ntp.org];

:local ntpipb [:resolve 1.ua.pool.ntp.org];

:if ($ntpipa != $ntpcura) do={/system ntp client set primary-ntp="$ntpipa";}

:if ($ntpipb != $ntpcurb) do={/system ntp client set secondary-ntp="$ntpipb";}”

Далі автоматизуємо процес оновлення часу кожні 12 годин, для цього створюємо розклад в планувальнику завдань:

/system scheduler add \

comment="Перевірка актуальності NTP-серверів" \

disabled=no \

interval=12h \

name=Check-NTP-servers \

on-event="/system script run Update NTP Server" \

policy=read,write,test \

start-date=jan/01/1970 \

start-time=07:00:00

4.5.2 Налаштування безпеки мережі

1) Прибираємо відповідь на запит PING з WAN портів.

Відповідь на запит PING значно підвищує ймовірність потрапити під приціл хакерів. За статистикою, якщо немає відповіді на PING-запит, то подальші спроби увійти за ip-адресу скорочуються на 40%.

Необхідно організувати заборону відповіді з WAN-портів для PING-запитів по опції echo reply і запитів по MAC адресу.

/ip firewall filter add chain=input action=drop protocol=icmp icmp-options=8:0 ininterface-list=WAN src-address-list="!Allow_IP_Remote_Management" comment=" Drop_input_echo_request"

/tool mac-server ping set enabled=no

2) Мережа інтернет составляесть ключову небезпеку для корпоративної мережі, тому що з відкритою постійно проходять спроби підключитися до стандартних портів популярних протоколів і служб.

Рішенням цієї проблеми буде виявлення і блокування всіх ip-адрес, з яких робляться спроби це зробити.

/ip firewall filter add chain=input action=add-src-to-address-list in-interfacelist=

WAN src-address-list="!Not_Drops_IP" protocol=tcp dstport=22, 23, 53, 389, 445, 3389, 4569, 5060, 5061, 8291 connection-nat-state=!dstnat address-list= Drop_Address address-list-timeout=3d comment="Drop TCP trafic"

Теж саме робимо і для трафіку UDP.

/ip firewall filter add chain=input action=add-src-to-address-list in-interfacelist=

WAN src-address-list="!Not_Drops_IP" protocol=tcp dstport=53, 161, 389, 4569, 5060 connection-nat-state=!dstnat address-list=Drop_Address

address-list-timeout=3d comment=" Drop UDP trafic"

За допомогою Firewall Raw блокуємо всі виявлені ip-адреси.

/ip firewall raw add action=drop chain=prerouting src-address-list=Drop_Address comment="Drop Address”

Створюємо «Білий список» ip-адрес.

/ip firewall address-list add address=192.168.0.0/24 list=Not_Drops_IP

Цим самим ми знизимо завантаження процесора в разі DOS-атак, бо з цим завданням справлятимуться Raw-таблиці, як наслідок роутер стане значно стійкіше до атаки типу «відмова в обслуговуванні».

3) Мережа постійно зазнає масовому скануванню портів, спеціальне програмне забезпечення зловмисників масово сканує пристрої глобальної мережі, і виявляють слабкі місця, після чого приступають до злому, що може бути ризиком уразливому пристрою стати частиною якоїсь нейромережі.

Для запобігання цієї проблеми необхідно прописати правило для виявлення сканування і подальшого блокування ip-адрес джерел запитів (рис. 4.8 - 4.10).

/ip firewall filter add chain=input action=add-src-to-address-list in-interfacelist=

WAN src-address-list="!Not_Drops_IP" protocol=tcp psd=10,10s,3,1 addresslist=

Drop_Address address-list-timeout=7d comment="Drop port scanning“

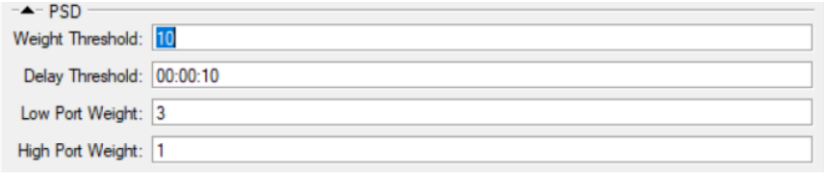

Рисунок 4.8 - Налаштування правила «Чорного списку»

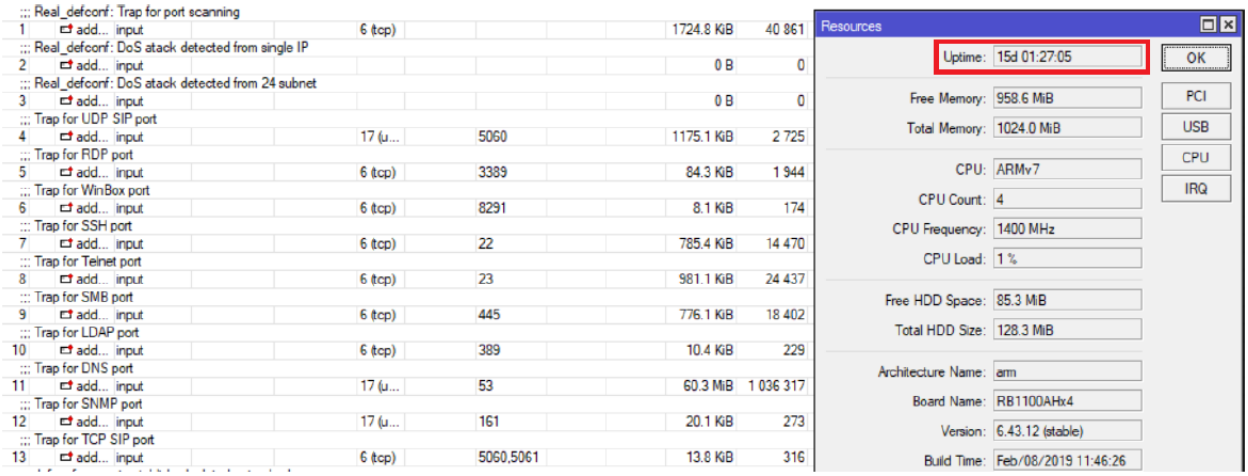

Рисунок 4.9 - Результати налаштування «Чорного списку»

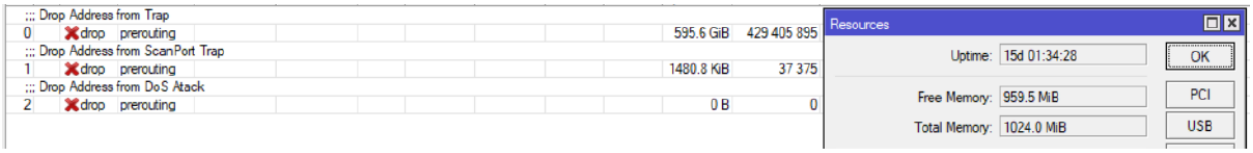

Рисунок 4.10 - Результати налаштування «Raw-таблиць»

4) Виключаємо можливість розсилки спама з нашої мережі.

Щоб виключити варіанти, коли заражені наші пристрої в мережі і спроби ними розсилати запити в зовнішню мережу, необхідно виявляти і заблокувати вірусну активність з внутрішньої мережі в мережу Інтернет, щоб не стати джерелом небезпеки для зовнішнього світу.

Для цього необхідно налаштувати блокування найбільш популярних для сканування портів з зовнішньої мережі (наприклад, порти 25, 587, 465), за винятком довірених хостів.

/ip firewall filter add action=drop chain=forward protocol=tcp dst-port=25,587,465 connection-state=new out-interface-list=WAN dst-addresslist=! SMTP-External-Servers src-address-list=!SMTP-Internal-Server-Clients log=yes log-prefix="SMTP Spam" comment=«Drop out SMTP not allow hosts“

/ip firewall filter add action=drop chain=forward protocol=tcp dst-port=445 connection-state=new out-interface-list=WAN log=yes log-prefix="SMB Scan" comment=“Drop out SMB not allow hosts"

Далі додаємо довірені адреси зовнішніх SMTP серверів, через які ми будемо надсилати листи.

/ip firewall address-list add address=smtp.gmail.com list=SMTP-External-Servers

/ip firewall address-list add address="mail.domain.com" list=SMTP-External-Servers

А також адреси внутрішніх SMTP серверів і клієнтів, які будуть мати право відправляти листи в світ.

/ip firewall address-list add address=192.168.0.4 list=SMTP-Internal-Server-Clients

5) Захист від атак типу «відмова в обслуговуванні».

Так само необхідно встановити додатковий захист своїх зовнішніх сервісів від атак типу DoS. Для цього ми будемо відловлювати і блокувати ip-адреси, які генерують занадто велику кількість з'єднань, для додавання блокуючого правила в firewall прописуємо наступні команди в консолі RouterOS.

/ip firewall filter add action=add-src-to-address-list address-list=DoS-Atack-Address address-list-timeout=1d chain=forward comment="DoS atack from single IP" connection-limit=20,32 connection-nat-state=dstnat in-interface-list=WAN

/ip firewall filter add action=add-src-to-address-list address-list=DoS-Atack-Address

address-list-timeout=1d chain=forward comment="DoS atack from 24 subnet" connection-limit=100,24 connection-nat-state=dstnat in-interface-list=WAN

6) Проблема немаршрутизованого трафіку.

У комп'ютерних мережах передається величезна кількість різних запитів, і не завжди вони позначені якоюсь конкретного адресою, тобто ми говоримо зараз про не маршрутизований трафік, так званих Bogon networks. З одного боку, за замовчуванням, маршрутизатор пропускає всі вихідні запити в світ, і якщо ви є великою компанією з величезною інфраструктурою, то ви можете пристойно засмічувати мережу провайдеру нікому не призначеними запитами, що не є добре.

А з іншого боку Bogon networks часто зловмисно використовується хакерами для своїх шкідливих атак. На цю проблему відреагувала організація Internet Engineering Task Force (IETF, укр. Інженерний рада Інтернету) і зробила список ip-адрес, рекомендованих до закриття на зовнішні інтерфейси приватних мереж.

За допомогою firewall блокуємо дані діапазони.

/ip firewall raw add action=drop chain=forward comment="Reject BOGONS IP" dst-address-list=BOGONS out-interface-list=WAN log=yes logprefix="BOGONS over WAN"

/ip firewall address-list

add address=0.0.0.0/8 list=BOGONS

add address=10.0.0.0/8 list=BOGONS

add address=100.64.0.0/10 list=BOGONS

add address=127.0.0.0/8 list=BOGONS

add address=169.254.0.0/16 list=BOGONS

add address=172.16.0.0/12 list=BOGONS

add address=192.0.0.0/24 list=BOGONS

add address=192.0.2.0/24 list=BOGONS

add address=192.168.0.0/16 list=BOGONS

add address=198.18.0.0/15 list=BOGONS

add address=198.51.100.0/24 list=BOGONS

add address=203.0.113.0/24 list=BOGONS

[16]

7) Організація резервних копій.

Необхідно завжди мати резервні копії конфігурації обладнання, а також відправляти ці бекапи на сторонній ресурс, наприклад, файлосховище або на електронну пошту. Ми розглянемо варіант з поштою, тому що ftp-сервера може не бути, а електронна пошта є у всіх.

Ні в якому разі не можна використовувати одну і ту ж пошту для відправки та отримання листів, необхідно щоб відправляючий поштовий ящик був створений саме для цієї мети і обов'язково автоматизуємо процес.

Для відправки електронної пошти потрібно налаштувати поштову скриньку, як зазвичай рекомендую використовувати командний рядок.

/tool e-mail set address=smtp.gmail.com from="mikrot_gw_backup" password=$ Email_Password port=465 start-tls=tls-only user=$Email_User_ Name

Пишемо скрипт для відправки повідомлення з backup-файлом.

/system script add name=Backup_to _email policy=read,write,policy,sensitive,test

source="/system backup save name=email_ backup;

:delay 5; /tool e-mail send file="email_ backup.backup"

to="it@company.com" from=mikrotik@company.com body="See attached file" subject="$[/system identity get name] $[/system clock get time] $[/system clock get date] Backup";

:delay 5; /file remove [find name="email_backup.backup"];”

Далі створюємо розклад в планувальнику завдань для запуску створеного вище скрипта.

/system scheduler add interval=1d name=Backup on-event="/system script run Backup_to_email” policy=read,write,policy,sensitive,test start-date=jan/01/1970

start-time=00:00:00

8) Налаштування системи керування трафіком (QoS).

У невеликих комерційних організаціях не так важливо обмежити швидкість, а більше пріоритезувати важливий трафік і мінімізувати вплив на нього другорядного трафіку. Але даний механізм привілейованості будуть діяти тільки для симетричних каналів.

Для початку виділяємо найбільш важливий трафік і маркуємо його.

/ip firewall mangle

#Трафік управління

add action=mark-connection chain=prerouting connection-state=new dstport=8291,22 new-connection-mark=ManagTraf passthrough=yes protocol=tcp

add action=mark-packet chain=prerouting connection-mark=ManagTraf_conn newpacket-mark=ManagTraf_Packets passthrough=no

#SIP-Трафік

add action=mark-connection chain=prerouting connection-state=new dst-addresslist=SIP_External_Servers new-connection-mark=SIP_Conn passthrough=yes srcaddress-list=SIP_Internal _Servers/Clients

add action=mark-connection chain=prerouting connection-state=new dst-addresslist=SIP_Internal_Servers/Clients new-connection-mark=SIP_Conn passthrough=yes src-address-list=SIP_External _Servers

add action=mark-packet chain=prerouting connection-mark=SIP_Conn new-packetmark=SIP_ Packet passthrough=no

#DNS-трафік

add action=mark-connection chain=prerouting connection-state=new dst-port=53 new-connection-mark=DNS_con passthrough=yes protocol=tcp

add action=mark-connection chain=prerouting connection-state=new dst-port=53 new-connection-mark=DNS_con passthrough=yes protocol=udp

add action=mark-packet chain=prerouting connection-mark=DNS_con new-packetmark=DNS _Packet passthrough=no

Трафік HTTP

add action=mark-connection chain=prerouting connection-state=new dstport=80, 443 new-connection-mark=HTTP_Con passthrough=yes protocol=tcp

add action=mark-packet chain=prerouting connection-mark=HTTP_Con new-packetmark=HTTP_Packet passthrough=no

Трафік RDP

add action=mark-connection chain=prerouting connection-state=new dst-port=3389

new-connection-mark=RDP_Con passthrough=yes protocol=tcp

add action=mark-packet chain=prerouting connection-mark=RDP_Con new-packetmark=RDP_ Packets passthrough=no

Інший трафік

add action=mark-connection chain=prerouting connection-state=new connection-mark=no-mark new-connection-mark=Other_traff_conn passthrough=yes comment="Other traffic connections"

add action=mark-packet chain=prerouting connection-mark=Other_traff_conn new-packet-mark=Other_traff_packets passthrough=no comment="$Other traffic packets"

Після необхідно створити чергу трафіку за пріоритетом:

/queue simple

add dst=ether1 name=ISP1 target=bridge1 total-max-limit="$InetSpeed"

add dst=ether1 name=SIP target=bridge1 packet-marks=SIP_Packet parent=ISP1 priority=1/1 total-queue=SIP total-max-limit=10M

add dst=ether1 name=ManTraff target=bridge1 packet-marks=ManagTraf_Packets parent=ISP1 priority=2/2 total-max-limit=10M

add dst=ether1 name=DNS target=bridge1 packet-marks=DNS_Packet parent=ISP1 priority=3/3 total-max-limit=10M

add dst=ether1 name=RDP target=bridge1 packet-marks=RDP_Packet parent=ISP1 priority=4/4 total-queue=pcq-download-default total-max-limit=10M

add dst=ether1 name=HTTP target=bridge1 packet-marks=HTTP_Packet parent=ISP1 priority=6/6 total-queue=pcq-download-default total-max-limit=10M

add dst=ether1 name=Other target=bridge1 packet-marks=Other_traff_packet parent=ISP1 priority=7/7 total-queue=pcq-download-default total-max-limit=10M

9) Налаштування VPN-сервера.

Для VPN-сервера на MikroTik обираємо протокол L2TP over IPSec, тому що він є одним з найбезпечніших протоколів VPN, досить простий в налаштуванні і VPN-клієнт вже є майже у всіх сучасних системах, як наслідок, немає необхідності встановлювати або налаштовувати якесь додаткове ПЗ, а просто потрібно згенерувати конфігураційний файл, наприклад, для генерації в ОС Windows використовуємо Connection Manager Administration Kit (CMAK), а для MacOS використовуємо Apple Configurator 2 і підключаємось.

В першу чергу створюємо новий інтерфейс.

/interface list add name=l2tp-in1 comment="VPN_Def_Conf”;

Додаємо пул адрес нашого VPN.

/ip pool add name="sklad-kh" ranges=10.10.11.0/24 comment="VPN_Def_Conf";

Запускаємо L2TP-сервер.

/interface l2tp-server server set enabled=yes default-profile=sklad-kh authentication=mschap2 use-ipsec=required ipsec-secret="$VPN_PSK" caller-idtype=number;

Налаштовуємо в Firewall правила проброcу портів.

/ip firewall filter{

add chain=input action=accept protocol=udp port=1701,500,4500 placebefore=[find where comment="drop all not from LAN"] comment="Allow port for L2TP server"

add chain=input action=accept protocol=ipsec-esp port=50 place-before=[find where comment="drop all not from LAN"] comment="Allow esp protocol for L2TP/Ipsec server"

};

Створюємо VPN користувача (рис. 4.11):

/ppp secret add name= sklad-kh password=passuser1 profile=sklad-kh service=l2tp

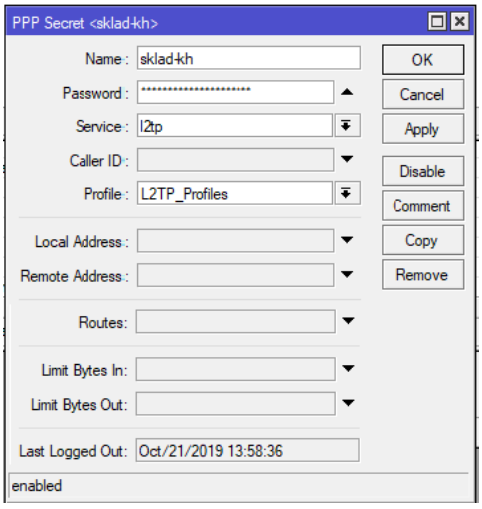

Рисунок 4.11 - Створення VPN користувача

Делее налаштовуємо параметри шифрування ipsec (рис. 4.12).

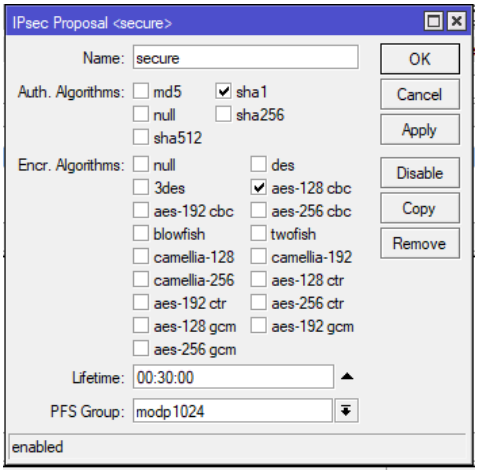

Рисунок 4.12 - Налаштування протоколів шифрування в ipsec

Генеруємо і встановлюємо необхідні сертифікати, створюємо з'єднання і прописуємо сертифікати (рис. 4.13).

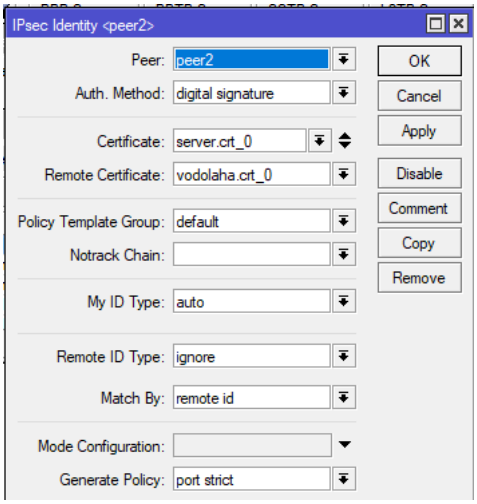

Рисунок 4.13 - Створення нового з’єднання, додавання сертифікатів

Далі додаємо l2tp клієнта на віддаленому маршрутизаторі, імпортуємо туди сертифікат і після проведених маніпуляцій отримуємо з'єднання з шифрованих трафіком (рис. 4.14).

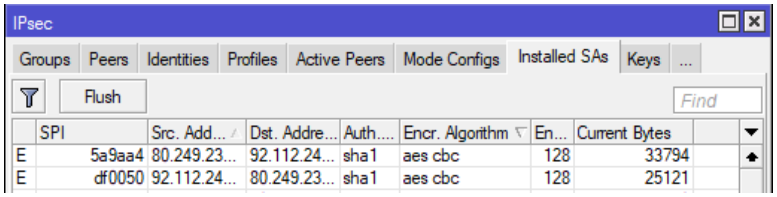

Рисунок 4.14 - Результат з’єднання 2-х мереж

10) Налаштування безшовного роумінгу за допомогою технології CAPsMAN.

Так як у кожного користувача в офісі є одне і більше пристроїв, що працюють з Wi-Fi, а якщо ці користувачі пересуваються по офісу, буде незручно перемикатися від точки до точки вручну, виходом з цієї проблеми буде налаштування технології CAPsMAN.

Система CAPsMAN призначена для централізованого управління декількома Wi-Fi точками доступу MikroTik. З її допомогою можна налаштувати для Wi-Fi точок одне ім'я мережі, пароль для підключення і реалізувати роумінг. Після внесення змін до настройки CAPsMAN, вони автоматично застосовуються до всіх Wi-Fi точок.

CAPsMAN налаштовується на будь-якому роутері MikroTik. Тобто роутер виступає в ролі контролера, а Wi-Fi точки підключаються до нього і отримують налаштування.

Повноцінний безшовний роумінг з відсутністю втрат переданих даних є тільки в дуже дорогому обладнанні з застосуванням апаратних контролерів. Однак в будинок, кафе, готель або невеликий офіс таке обладнання можуть дозволити собі далеко не всі.

У недорогих рішеннях, як у MikroTik, роумінг відбувається з не великими затримками і втратами даних. Наприклад, при розмові по Skype або Viber при переході від точки до точки на 1-2 секунди може зависнути звук. Якщо ви качаєте файл з сайту, який не підтримує докачку, то при переході станеться обрив, і закачування доведеться виконати заново. При перегляді відео з Youtube перемикання буде непомітно, оскільки дані кешуються. При серфінгу в браузері перемикання так само непомітно.

Почнемо з налаштування частот.

/caps-man channel {

add band=2ghz-b/g/n control-channel-width=20mhz extensionchannel=disabled frequency=2412 name=channel1 reselectinterval=1d tx-power=20}

Налаштуємо профіль безпеки:

/caps-man security add authentication-types=wpa2-psk encryption=aes-ccm groupencryption=aes-ccm disable-pmkid=yes name=security1 passphrase="$PassOffice"

Налаштуємо правила потоку трафіку:

/caps-man datapath add client-to-client-forwarding=yes local-forwarding=yes name=OfficeNet

Створимо конфігурації для застосування на WiFi точках:

/caps-man configuration {

add channel= channel1 datapath=datapath1

distance=indoors guard-interval=long max-sta-count=32 mode=ap multicasthelper=default name=cfg1 rates=StandartDataRates rx-chains=0,1,2 security=security1 ssid="$SSIDOffice" tx-chains=0,1,2}

Налаштовуємо автоконфігурації в мережі:

/caps-man provisioning {

add action=create-disabled hw-supported-modes=gn masterconfiguration=cfg1 name-format=cap }

І вмикаємо CAPsMAN.

/caps-man manager set enabled=yes

Налаштування CAP.

/system reset-configuration caps-mode=yes

Після перезавантаження обладнання встановлюємо зрозуміле ім'я.

/system identity set name=“CAP1”

Для безпеки необхідно встановити логін і пароль і відключити все зайве.

Залишається тільки включити створені при автоконфігурації інтерфейси на контролері.

11) Налаштування гостьової точки доступа.

Не всім Wi-Fi користувачам необхідний доступ до корпоративної мережі, багатьом достатньо простої наявності мережі Інтернет, не кажучи вже щодо можливих гостей компанії, їм доступ в мережу необхідно заборонити. Для цього створимо нову підмережу з доступом тільки в Інтернет.

Налаштуємо на вже створеному CAPsMAN гостьову WiFi мережу з доступом тільки в Інтернет.

Створимо окремий гостьовий bridge:

/interface bridge add name=bridge-guest;

/ip address add address=192.168.11.1/24 interface=bridge-guest;

Нам потрібен окремий DHCP сервер на гостьовому bridge:

/ip pool add name="guest-pool" ranges=192.168.11.2-192.168.11.100;

/ip dhcp-server add name=dhcp-guest address-pool="guest-pool" interface=bridge-guest lease-time=1h disabled=no;

/ip dhcp-server network add address=192.168.11.0/24 gateway=192.168.11.1;

Направляємо всіх гостей в окрему таблицю маршрутизації і створюємо мінімальний набір маршрутів:

/ip route rule add action=lookup-only-in-table interface=bridge10 table=MG-Guest;

/ip route {

add dst-address192.168.11.0/24 gateway=bridge-guest routing-mark= MG-Guest;

add dst-address="$WANIP/$WANIPprefix" gateway=ether1 routing-mark= MG-Guest;

add dst-address=0.0.0.0/0 gateway="$WANGW" routing-mark= MG-Guest;

}

Перейдемо до налаштувань CAPsMAN. Налаштування каналів, модуляцій і листи доступу у нас вже є. Нам потрібні налаштування потоку даних, в них ми забороняємо точкам самим вирішувати куди відправляти трафік і залишаємо це навантаження за контролером, забороняємо спілкування клієнтів між собою:

/caps-man datapath add bridge=bridge-guest client-to-client-forwarding=no localforwarding= no name= datapath2

Профіль безпеки:

/caps-man security add authentication-types=wpa2-psk encryption=aes-ccm groupencryption=aes-ccm disable-pmkid=yes name=security_guest passphrase="$PassGuest"

Профіль конфігурації:

/caps-man channel {

add band=2ghz-b/g/n control-channel-width=20mhz extensionchannel=disabled frequency=2437 name=channel2 reselectinterval=1d tx-power=20/caps-man configuration }

/caps-man configuration {

add channel=channel2 datapath=datapath2 distance=indoors guard-interval=long max-sta-count=32 mode=ap multicasthelper= default name= cfg2 rates=StandartDataRates rx-chains=0,1,2 security=GuestNetPass ssid="$SSIDOffice-Guest" tx-chains=0,1,2}

Додаємо конфігурації до нашого автоналаштування в CAPsMAN:

/caps-man provisioning {

set [find master-configuration=cfg1] slaveconfigurations=cfg2};

Вмикаємо CAPsMAN:

/caps-man manager set enabled=yes

Налаштування CAP:

/system reset-configuration caps-mode=yes

Після перезавантаження обладнання встановлюємо зрозуміле ім'я:

/system identity set name="CAP2"

Все те саме повторюємо і для інших точок, результат можно побачити на рисунках 4.15 - 4.16.

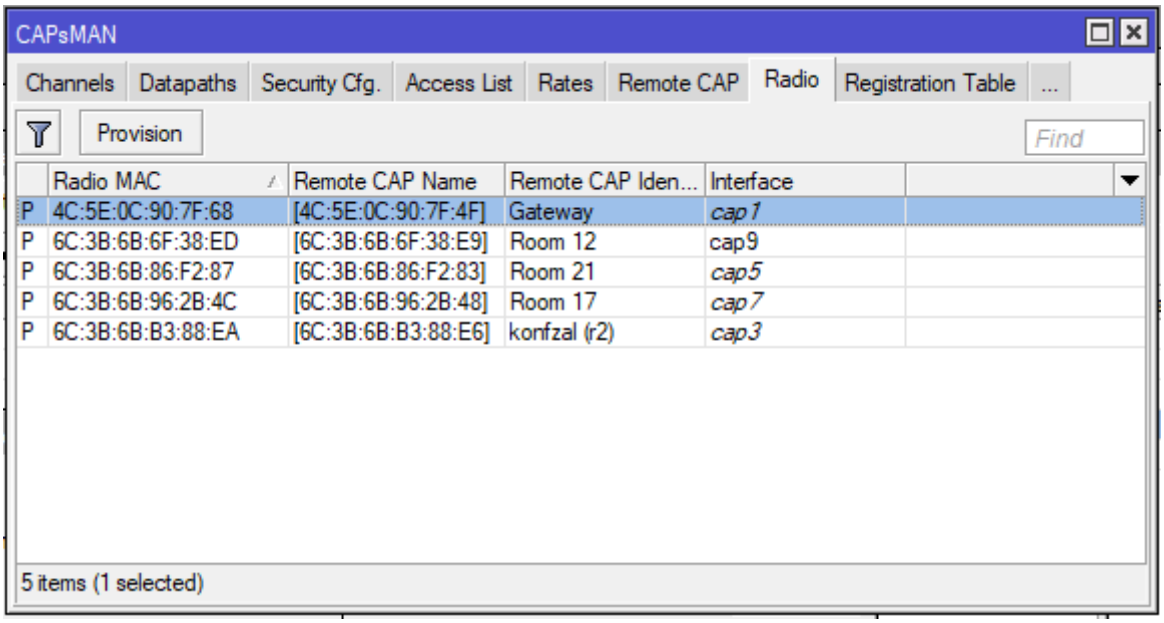

Рисунок 4.15 - Список доданих точок до загального безшовного роумінгу

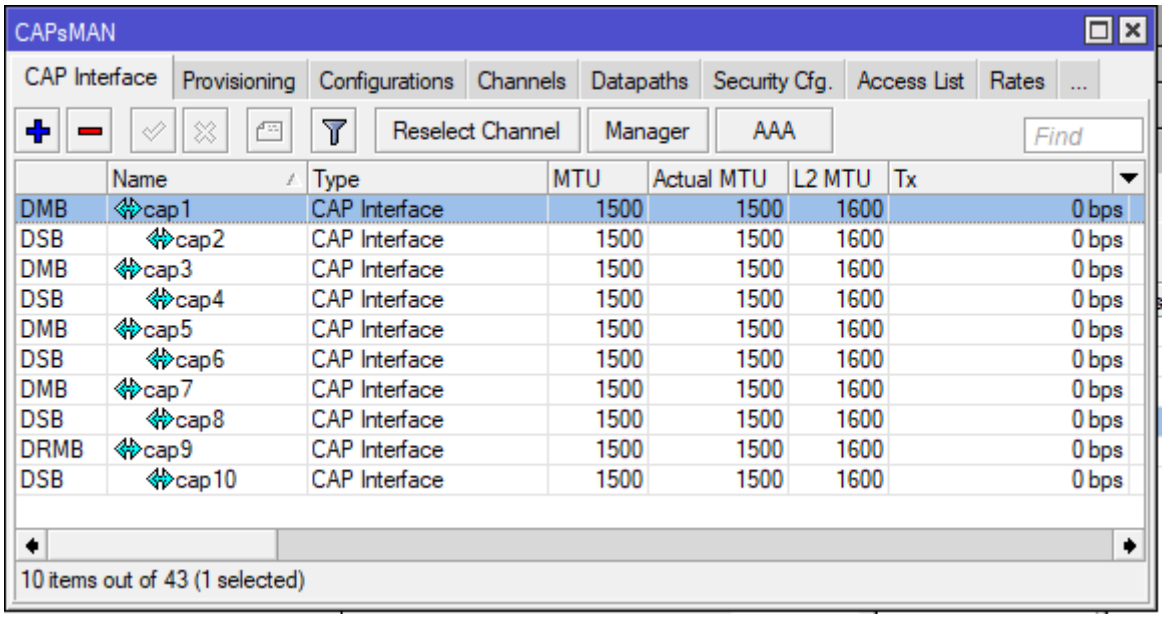

Рисунок 4.16 - Список доданих Wi-Fi точок гостьової і локальної мережі

4.5.3 Використання скриптів автоматичного налаштування.

Які переваги ми при цьому отримуємо:

1) Економія часу – те що в ручному режимі роботи, при умові відсутності помилок, займе годину-дві, за допомогою підготованого скрипта, цей час зменшується до 10 хвилин, тобто економія часу – 80-90%.

2) Гарантія відсутності помилок – при ручному налаштуванні може виникнути так званий «людський фактор», тобто людина може допустити помилку або просто забути увімкнути якусь опцію. Крім того, як показує практика, копіювання також може виконуватись некоректно і створювати додаткові помилки. В кращому разі це спричинить тільки те, що правило не виконається, а може спрацювати так, що воно виконається з помилками, а це вже може бути геть інший результат, ніж той, на який ми сподівалися.

Розглянемо як ними користуватись. По перше створюэмо текстовий файл, куди записуємо наш скрипт і зберігаємо його в форматі *.rsc, після чого його потрібно скопіювати у внутрішню пам’ять маршрутизатора (Рис. 4.17).

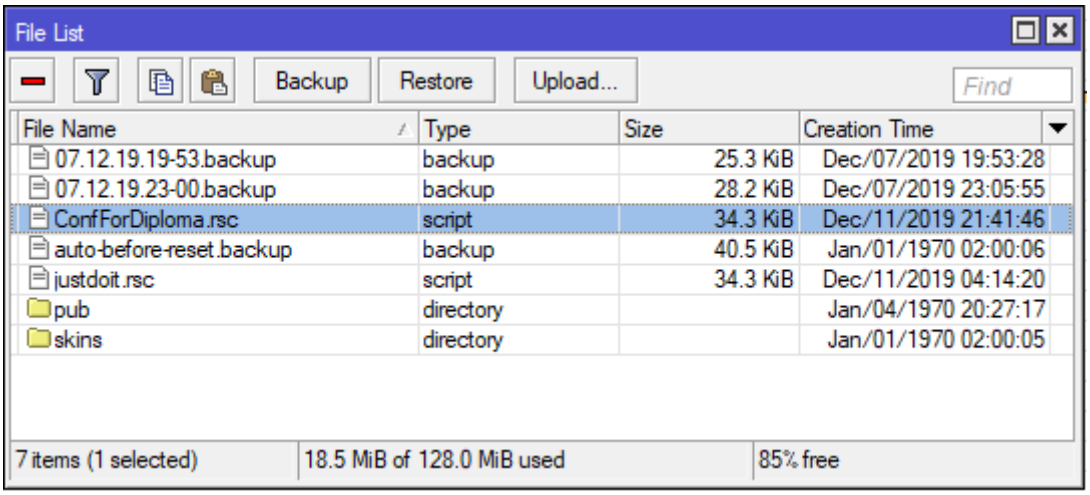

Рисунок 4.17 - Додавання файлу скрипта до внутрішньої пам’яті маршрутизатора

І запустити із командного рядка команду (Рис. 4.18).

/import name-script-file.rsc

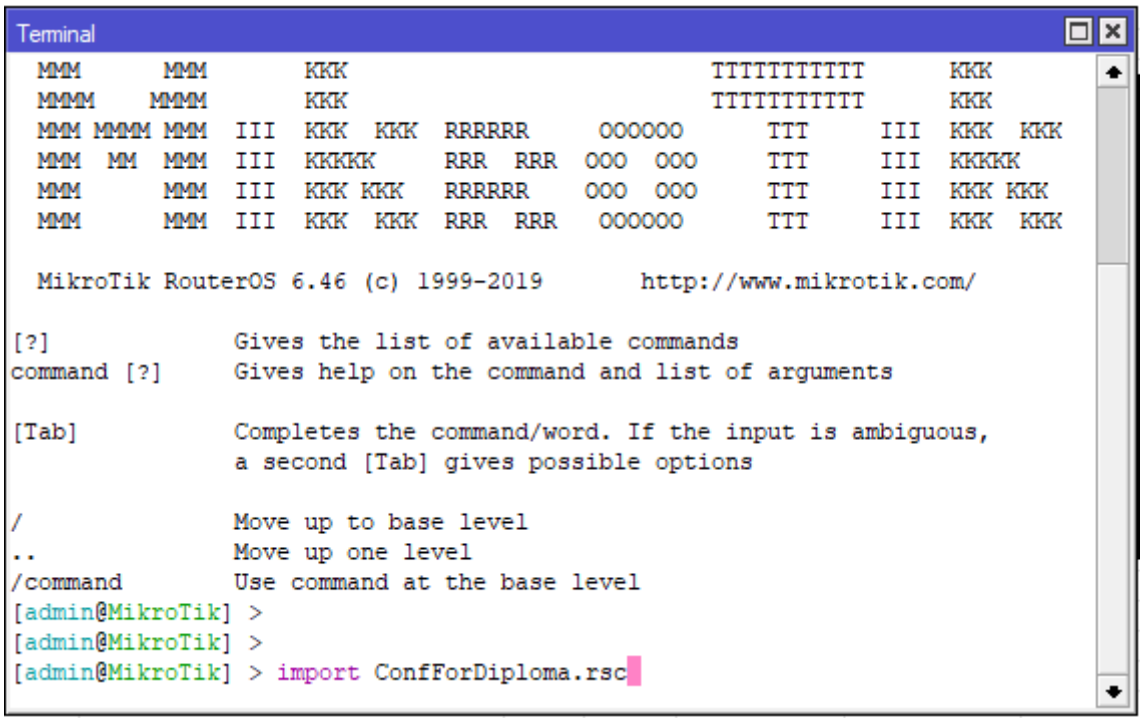

Рисунок 4.18 - Виконання команди запуску скрипта

Після чого отримуємо результат:

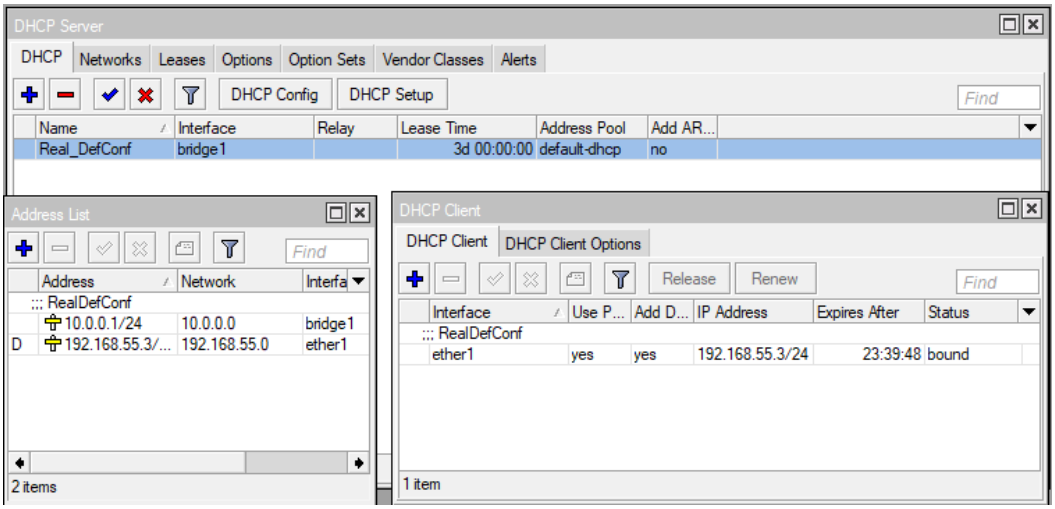

Рисунок 4.19 - Результат роботи виконання скрипта в отриманні зовнішньої адреси і запуску DHCP-сервера

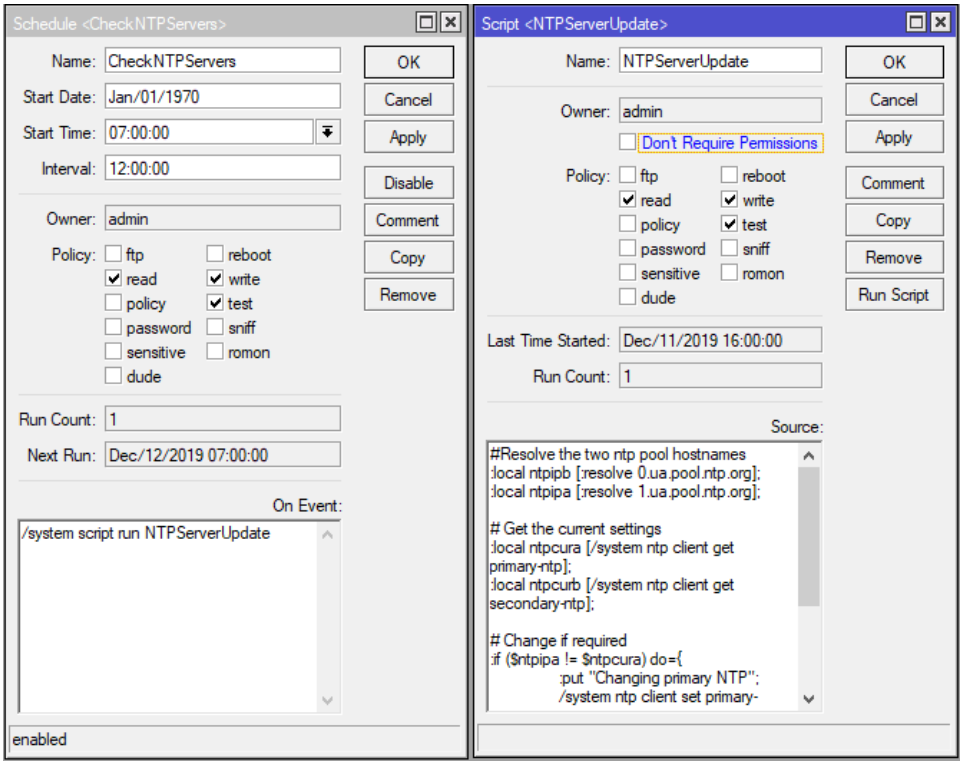

Рисунок 4.20 - Результат роботи виконання скрипта в налаштуванні часу

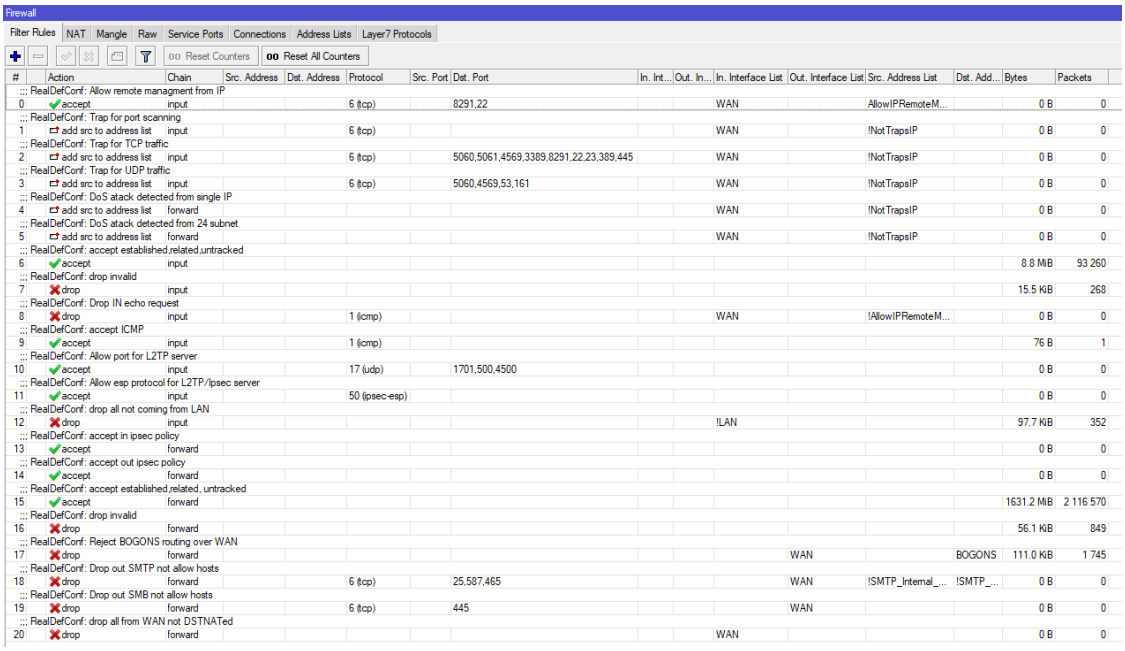

Рисунок 4.21 - Результат роботи виконання скрипта у мережевому екрані

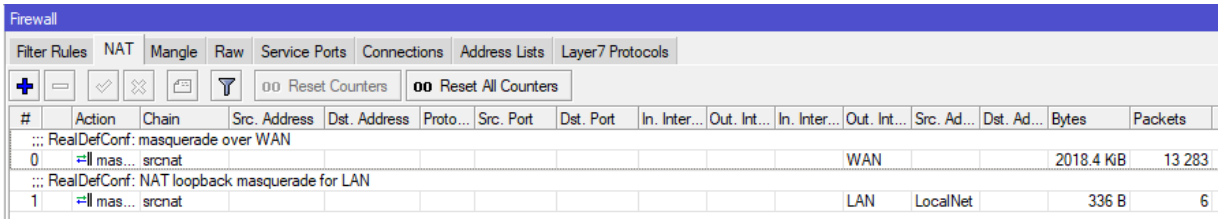

Рисунок 4.22 - Результат роботи виконання скрипта в налаштуваннях NAT

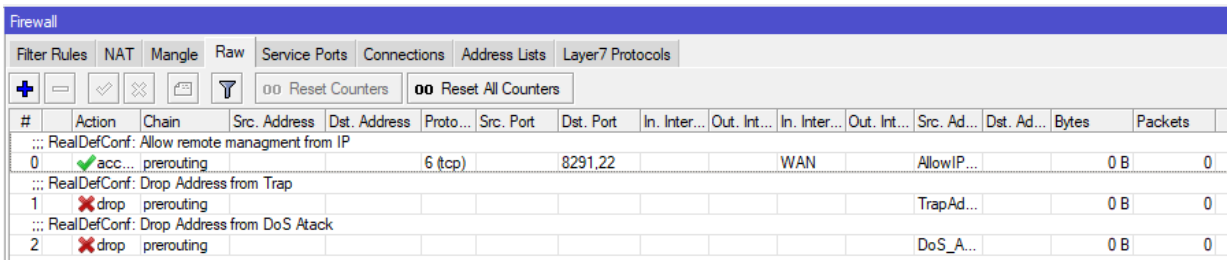

Рисунок 4.23 - Результат роботи виконання скрипта у Raw-таблицях

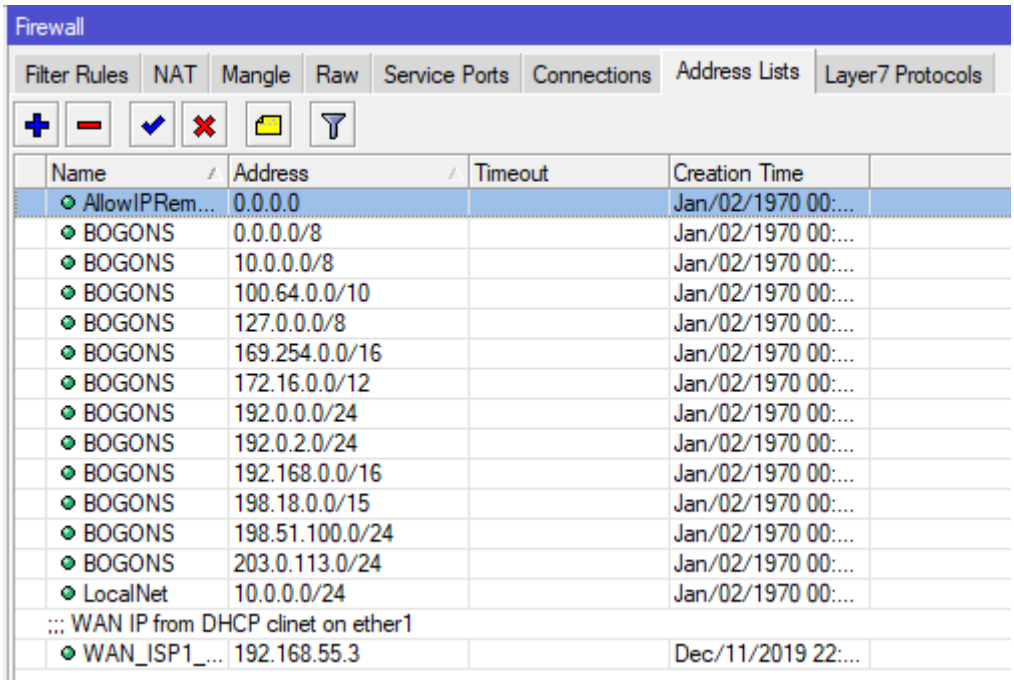

Рисунок 4.24 - Результат роботи виконання скрипта у створенні списків адрес

Повний скрипт налаштувать дивитись у додатку А.

4.6 Тестування на проникнення в налаштовану систему

Для того щоб перевірити надійність налаштованої нами системи захисту, необхідно провести аудит нашої комп’ютерної мережі.

Організація повинна проводити внутрішній аудит СМІБ в заплановані інтервали для визначення, чи відповідають мета, засоби управління, процеси та процедури СМІБ наступним положенням:

- відповідність вимогам Міжнародного стандарту і відповідним нормативним та установчим актам;
- відповідність ідентифікованим вимогам ІБ;
- ефективне забезпечення і підтримка СМІБ.

Основними видами аудиту ІБ є:

- експертний аудит ІБ, під час якого виявляються недоліки у системі заходів ЗІ на основі досвіду експертів, що беруть участь у процедурі аудиту;
- аудит ІБ на відповідність міжнародним стандартам, наприклад, стандарту ISO/IEC 27001 «Інформаційні технології. Методи забезпечення безпеки. Системи менеджменту інформаційної безпеки. Вимоги»;
- активний аудит, головним завданням якого є оперативне виявлення підозрілої активності і надання засобів для автоматичного реагування на неї. Під підозрілою активністю розуміють поведінку користувача або компоненти інформаційної системи, яка є зловмисною (відповідно до заздалегідь визначеної політики безпеки) або нетиповою (згідно з прийнятими критеріями). активний аудит, крім того, дозволяє запрограмувати реакцію на порушення з метою локалізації та / або простежування;
- комплексний аудит, що включає в себе всі перераховані вище форми проведення обстеження.

В нашому випадку ми будемо проводити саме активний аудит, в ході якого ми змоделюємо декілька атак, а виходячи з того, чи будуть ці атаки успішними, зможемо зробити висновок, безпечна запропонована система захисту, чи ні.

Для моделювання атаки будемо використовувати дистрибутив сімейства Linux, а саме систему Kali Linux, яка включає одну з найповніших добірок інструментів для фахівців в області комп'ютерної безпеки: від засобів для тестування web-додатків і проникнення в бездротові мережі, до програм для зчитування даних з ідентифікаційних RFID чіпів.

Ми з тестованим пристроєм знаходимося в підмережі 192.168.0.0/24. Наша IP-адреса: 192.168.0.102 (рис. 4.25).

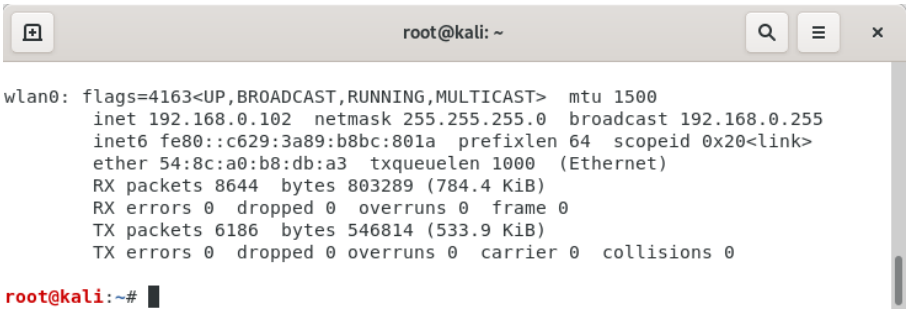

Рисунок 4.25 - IP-адреса тестуючого пристрою

Аудит проводимо з точки зору зловмисника, метою якого є проникнення у корпоративну мережу організації:

1) Шукаємо усі MAC-адреси пристроїв в мережі за допомогою команди: arp -a. (Рис. 4.26)

Рисунок 4.26 - Пошук MAC-адрес в підмережі

2) Намагаємося дізнатися ip-адреса пристрою по MAC-адресу, для цього використовуємо пінг MAC-адреси: arping 74:4d:28:87:9c:d6 (рис. 4.27).

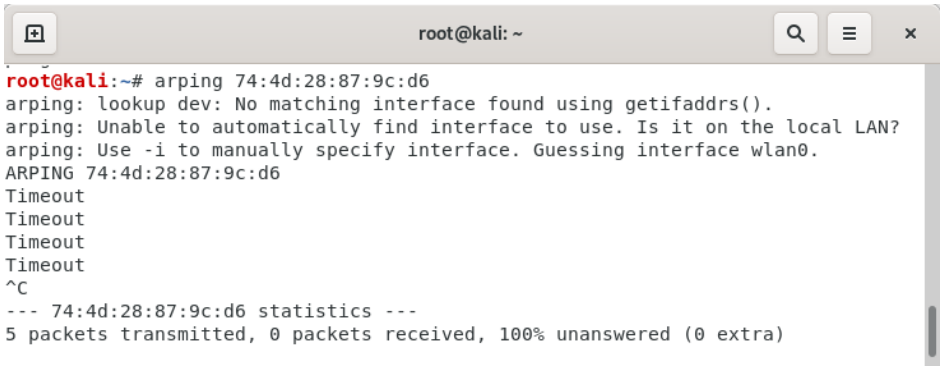

Рисунок 4.27 - Пінг MAC-адреси

Пристрій нам не відповів, це означає, що пінг за MAC-адресою на ньому відключений і ці налаштування вже спрацювали на нашу користь.

3) Наступним кроком, за допомогою програми Nmap робимо сканування підмережі на фізичні і локальні адреси (рис. 4.28).

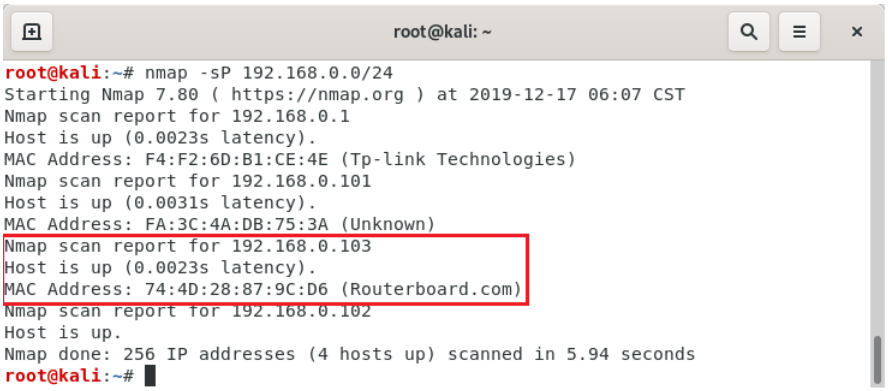

Рисунок 4.28 - Сканування пристроїв в мережі

Отримуємо ip-адресу тестованого пристрою: 192.168.0.103. Перевіряємо наш чи це маршрутизатор (рис. 4.29).

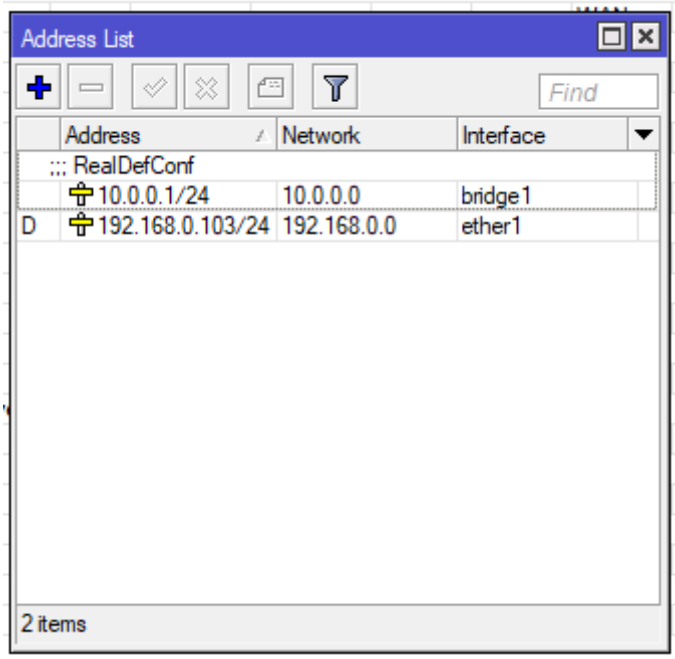

Рисунок 4.29 - Перевірка ip-адреси

Як бачимо 192.168.0.103 - це адреса тестованого пристрою.

4) Знову ж таки, за допомогою програми Nmap скануємо тестований маршрутизатор на відкриті порти і встановлену ОС (рис. 4.30).

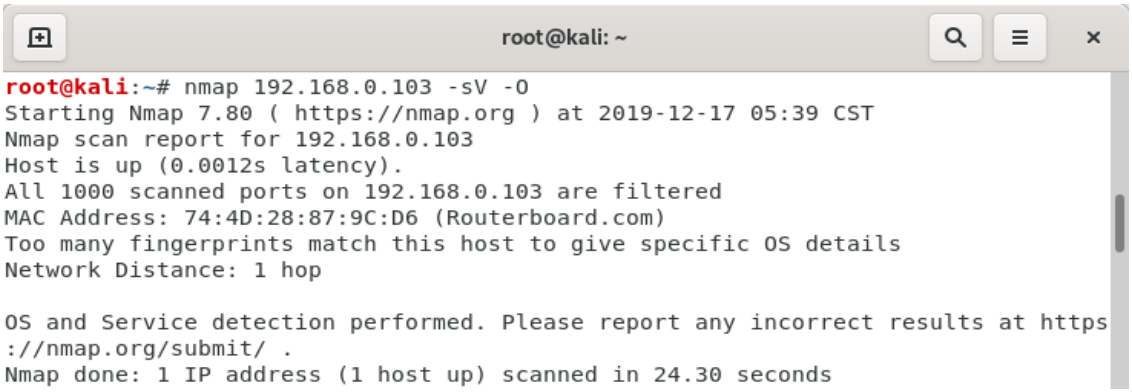

Рисунок 4.30 - Результат виконання сканування відкритих портів.

Відображається результат, що відкритих портів не було виявлено і відразу ж, додається ip-адреса тестуючого пристрою в чорний список тестованого пристрою і вказується кількість адрес, що намагались вчинити сканування портів (рис. 4.31).

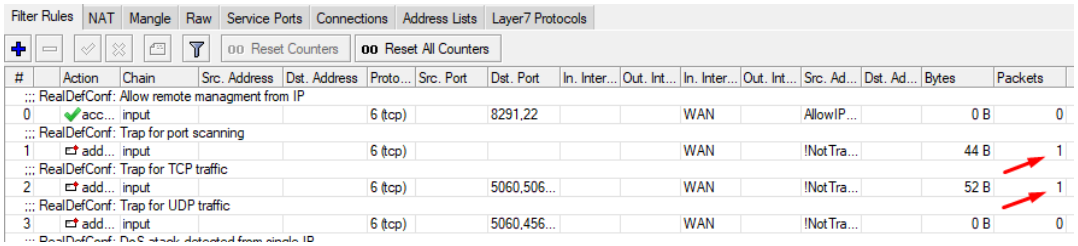

Рисунок 4.31 - Виявлення числа порушників

Перевіряємо, чия адреса була занесена до чорного списку (рис. 4.32).

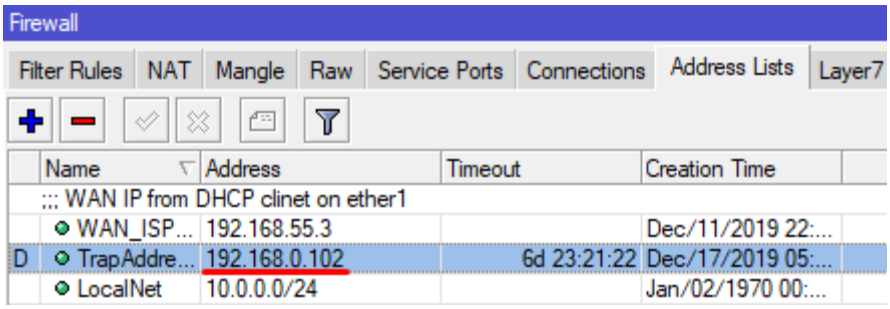

Рисунок 4.32 - Визначення адреси за автоматично внесеними змінами в Address list

Виходячи з того, стандартними засобами майже нічого не вдалось з'ясувати, спробуємо використати спеціальні засоби призначені саме для аудиту комп'ютерних мереж, а саме утіліту Router Scan, процес запуску якої показано на рисунку 4.33.

Рисунок 4.33 – Запуск утіліти Router Scan

Router Scan – це утіліта, що призначена для аудиту комп'ютерних мереж, як локальних, так і глобальних.

Принцип роботи: утіліта Router Scan знаходить і визначає різні пристрої з великого числа відомих роутерів / маршрутизаторів. Отримує від них корисну інформацію, зокрема характеристики бездротової мережі: спосіб захисту точки доступу (шифрування), ім'я точки доступу (SSID) і ключ точки доступу (парольний фраза). Також отримує інформацію про WAN-з'єднання (зручно при скануванні локальної мережі) і виводить марку і модель роутера. Отримання інформації відбувається за двома можливими шляхами: програма спробує підібрати пару логін / пароль до маршрутизатора зі списку стандартних паролів, в результаті чого отримає доступ. Або будуть використані неруйнівні уразливості (тобто ті, що істотно не вплинуть на роботу маршрутизатора) для конкретної моделі маршрутизатора, що дозволяють отримати необхідну інформацію та / або обійти процес авторизації.

Перейдемо до процесу сканування. Поперше видалимо нашу ip-адресу з чорного списку маршрутизатора, далі приступаємо до налаштувань программи аудиту, а саме вказуємо підмережу в якій знаходиться тестуємий маршрутизатор: 192.168.0.0/24, вмикаємо всі можливі скануючі модулі, задля більшої вірогідності позитивного результату, а також додаємо всі необхідні для сканування порти, дивись рисунок 4.34.

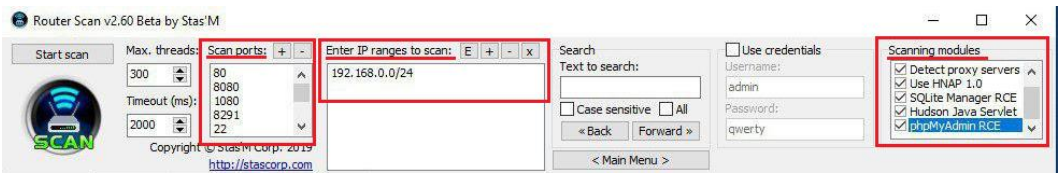

Рисунок 4.34 – Налаштування утіліти Router Scan

Поглянемо на результат сканування на рисунку 4.35, задля того, щоб зберегти чистоту експеременту ми тимчасово вмикаємо видимість маршрутизатора Mikrotik, під екраном сканування за допомогою програми управління, ми бачимо дійсну ip-адресу в реальному режимі часу. При цьому в результатах сканування тестованої мережі нашого маршрутизатора виявлено не

було, зате було виявлено інший маршрутизатор, на прикладі якого можно пересвідчитися в дієвості цієї програми для аудиту.

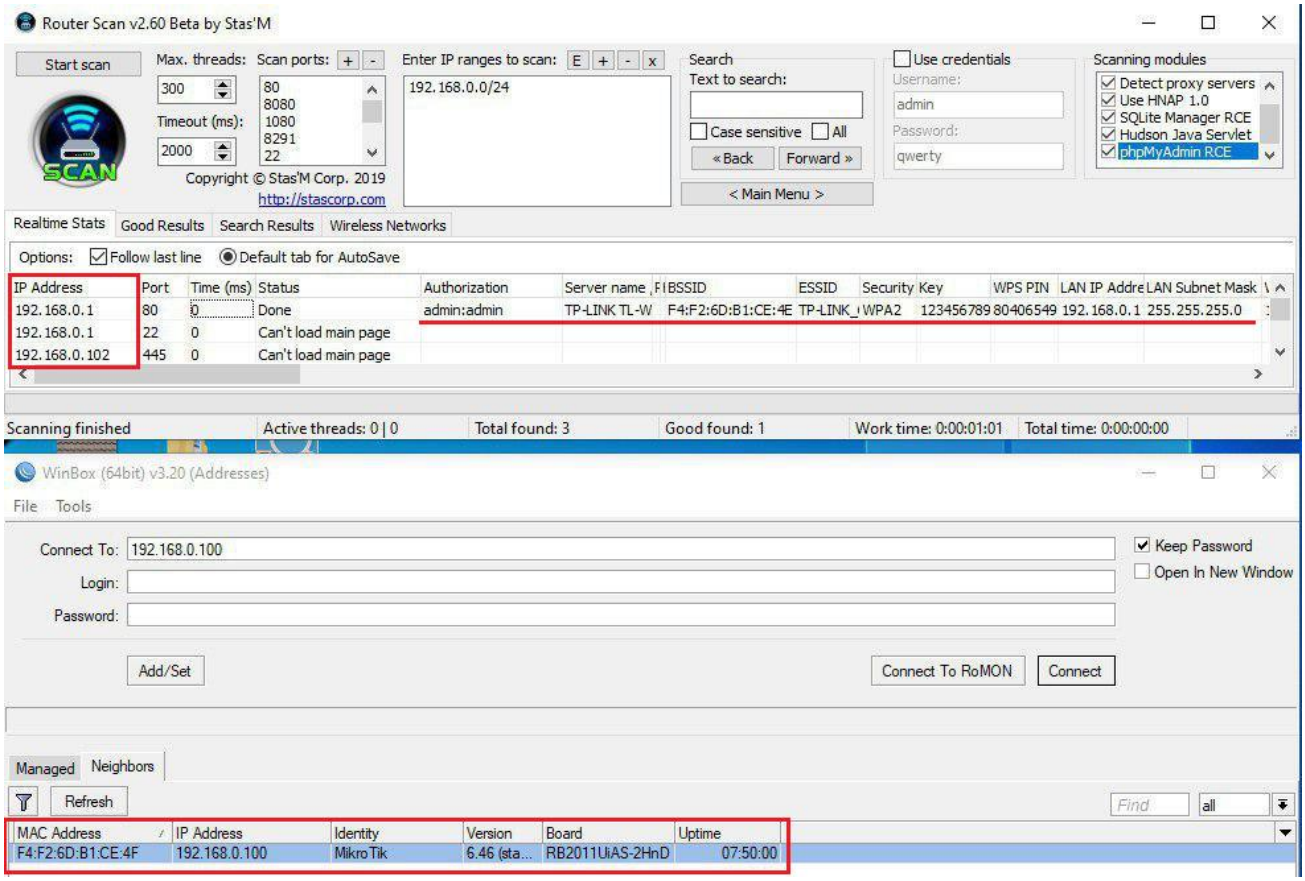

Рисунок 4.34 – Сканування мережі утілітою Router Scan

Виходячи з цього можна зробити висновок, що система безпеки функціонує, фільтрація пакетів виконується і маршрутизатор запобіг можливість атаки на функціонуючу за ним мережу.

ВИСНОВОК

В дипломній роботі розв’язана задача удосконалення методів та засобів підвищення безпеки комп’ютерних мереж. При цьому отримані наступні результати:

- проведено аналіз та порівняння існуючих мережевих загроз та методів захисту мереж;
- проаналізовано та запропоновано апаратно-програмні засоби та аспекти організації мережевої безпеки.
- проаналізовано можливості та вразливості обраного апаратно-програмного засобу;
- проведений аудит комп’ютерної мережі, в основі якої встановлений маршрутизатор MikroTik;
- запропоновано запровадження переліку налаштувань головного маршрутизатора задля забезпечення максимального захисту локальної мережі та розроблений для цього скрипт автоматичного налаштування.

Завдання створення ефективних інтегрованих систем захисту комп'ютерної мережі може бути вирішено за допомогою набору методів і технологій, реалізованих в сучасному телекомунікаційному обладнанні, такому як mikrotik, cisco, juniper, ubiquiti, тощо. За умови розумного проектування системи безпеки в організації такий підхід дозволяє ефективно протидіяти порушенню інформаційної безпеки за невеликі кошти.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Оглтрі Т.В. Firewalls. Практичні застосування міжмережевих екранів. «ДМК», М., 2008. - 109 с .;

2. Бірюков А.А. Інформаційна безпека: захист і напад. 2-ге вид. «ДМК-Пресс», М., 2017. – 347 с.

3. Аудит інформаційної безпеки навч. посібник для вузів / В.І. Аверченков. – 3-те вид. – М.: ФЛІНТА, 2016. – 269 с.

4. Біячуев Т.А. Безпека корпоративних мереж. СПб., 2008. - 327 с.;

5. Щеглов А.Ю. Захист комп'ютерної мережі від несанкціонованого доступу. «НиТ», СПб., 2009. - 202 с.;

6. Зіглер Р. Брандмауери в Linux. «Вільямс», М., 2009. - 74 с .;

7. Яковлєв В.Ю. Міжмережеві екрани, Спб., 2009. - 32 с .;

8. Ubiquiti vs Mikrotik: веб-сайт. URL: https://forum.mikrotik.com/viewtopic.php?t=82501#p415257 (дата звернення: 15.12.2019);

9. Mikrotik Router OS - описание и возможности: веб-сайт. URL: https://lanmarket.ua/stats/mikrotik-router-os-opisanie-i-vozmozhnosti/ (дата звернення: 15.12.2019);

10. За что я люблю и ненавижу MIKROTIK: веб-сайт. URL: https://mum.mikrotik.com/presentations/MD19/presentation_7212_1568363147.pdf (дата звернення: 15.12.2019);

11. Спецификация MikroTik RB4011iGS+RM: веб-сайт. URL: https://mikrotik.com/product/rb4011igs_rm#fndtn-specifications (дата звернення: 15.12.2019);

12. Ubiquiti EdgeRouter 12P (ER-12P) Маршрутизатор: веб-сайт. URL: http://ubiquiti.net.ua/ubiquiti-edgerouter-12p-er-12p?keyword=Ubiquiti%20EdgeRouter%2012 (дата звернення: 15.12.2019);

13. CVE's for routeros: веб-сайт. URL: http://cve.circl.lu/search/mikrotik/routeros (дата звернення: 15.12.2019);

14. Немаршрутизируемые в Интернет адреса (bogon networks) и безопасность: веб-сайт. URL: https://www.securitylab.ru/blog/personal/aodugin/305208.php (дата звернення: 15.12.2019).